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 126-146

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.

CROATIA

1. Legal Sources

As will be demonstrated in the chapters to follow, Croatia belongs to the **category of countries with some, sector-specific and fragmentary regulation** on issues of blocking, filtering and the taking down of illegal internet content. However, there are various legal sources, international, otherwise supranational and national, which do contain certain rules related to such measures. The most pertinent provisions may be found in the context of the **criminal procedure** regulatory scheme, operations of the providers of electronic communication services and **internet service provider operations** as well as in the context of **intellectual property rights enforcement**.

The **Constitution** of the Republic of Croatia[1] is the fundamental legal source in the Croatian legal system. Article 5(1) lays down that Croatian Acts shall conform to the Constitution, and other rules and regulations shall conform to the Constitution and the Acts. This equally applies to the Acts and rules which regulate laws and regulations related to the Internet. Furthermore, the Constitution presents the legal framework for the interpretation of these Acts and rules.

International treaties constitute an important source of the Croatian law. The provision of Article 140 of the Croatian Constitution prescribes as follows: "International agreements concluded and ratified in accordance with the Constitution and made public, and which are in force, shall be part of the internal legal order of the Republic of Croatia and shall be by its legal force above Acts." International conventions and treaties signed by the Republic of Croatia subsequent to 8 October 1990 – the date when Croatia's independence declaration came into effect and Croatia became a sovereign state – if ratified and publicized according to the prescribed rules, make part of its internal legal order. This is equally true for the conventions and treaties to which the former Yugoslavia was a party, which continued to be in force in Croatia on the basis of succession.

A number of multilateral and bilateral treaties in the field of the internet are in force in Croatia. In particular, Croatian law relating to blocking, filtering and take-down of illegal internet content is strongly influenced by international legal instruments and EU legislation. The list provided below is by no means exhaustive, but contains only some of the international treaties concluded under the auspices of the Council of Europe pertinent to the topic of the report:

- Convention on Cybercrime,[2]
- Additional Protocol to the Convention on Cybercrime,[3]
- Convention on the Prevention of Terrorism,[4]
- Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse,[5] (communication technologies mentioned several times regarding criminalisation of acts using them and regarding their use in preventing or punishing crimes),

---

1 The Constitution of the Republic of Croatia, Official Gazette of the Republic of Croatia nos. 85/2010(consolidated version) and 5/2014.

2 Official Gazette of the Republic of Croatia – International Treaties nos. 9/2002 and 4/2004.

3 Official Gazette of the Republic of Croatia – International Treaties no. 4/2008.

4 Official Gazette of the Republic of Croatia – International Treaties nos. 10/2007 and 1/2008. For instance, the act of "public provocation to commit a terrorist offence" as included in the Convention Article 5 is criminalised by means of Article 99 of the Criminal Act titled "Public Incitement to Terrorism". Also criminalised is the act of "Public Incitement to Violence and Hatred" in Article 325 of the Criminal Act.

5 Official Gazette of the Republic of Croatia – International Treaties nos. 11/2011, 13/2011 and 15/2011.

- Convention for the protection of individuals with regard to automatic processing of personal data.[6]

Some of the EU legal instruments include:

- 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,[7]
- Council Framework Decision of 13 June 2002 on combating terrorism,[8]
- Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA,[9]
- Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights,[10]
- Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'),[11]
- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data,[12]
- Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws.[13]

Among many relevant Croatian national acts, it seems important to mention:

- Republic of Croatia Security-Intelligence System Act[14]
- Data Secrecy Act,[15]
- Personal Data Protection Act,[16]
- Criminal Act,[17]
- Criminal Procedure Act,[18]
- State Inspectorate Act,[19]
- Copyright and Related Rights Act,[20]

---

6 Official Gazette of the Republic of Croatia – International Treaties nos. 4/2005, 6/2005 and 12/2005.
7 Official Journal L 335/1, 17.12.2011.
8 Official Journal L 164/3, 22.6.2002.
9 Official Journal L 218/8, 14.8.2013.
10 Official Journal L 157/45, 30.4.2004 and 195/16, 2.6.2004 (corrigendum).
11 Official Journal L 178, 17.7.2000.
12 Official Journal L 281/31, 23.11.1995.
13 Official Journal L 337/11, 18.12.2009.
14 Official Gazette of the Republic of Croatia nos. 79/2006 and 105/2006.
15 Official Gazette of the Republic of Croatia nos. 79/2007 and 86/2012.
16 Official Gazette of the Republic of Croatia nos. 103/2003, 118/2006, 41/2008 and 130/2011.
17 Official Gazette of the Republic of Croatia nos. 125/2011, 144/2012, 56/2015 and 61/2015.
18 Official Gazette of the Republic of Croatia nos. 152/2008, 76/2009, 80/2011, 91/2012, 143/2012, 56/2013, 145/2013 and 152/2014.
19 Official Gazette of the Republic of Croatia nos. 116/2008, 123/2008, 49/2011, 148/2013, 14/2014 and 19/2014.

- Patent Act,[21]
- Trademark Act,[22]
- Industrial Design Act,[23]
- Enforcement Act,[24]
- Electronic Communications Act.[25]

2. Legal Framework

2.1. Blocking and/or filtering of illegal Internet content

In Croatia there is **no specific legislation** which would regulate blocking and/or filtering of illegal Internet content.

2.1.1. Blocking and filtering in educational institutions

Filtering of Internet content is operated in educational institutions based on the Decision by the Ministry of Science, Education and Sports.[26] This Decision institutes obligatory content blocking /filtering for primary and secondary schools and optional blocking/filtering for institutions of higher education, such as universities. All primary and secondary schools connected to the Croatian Academic and Research Network (CARNet)[27] are automatically subject to the filtering system aimed at preventing access to unmoral content. This Decision prevents display of internet pages falling under any of the 14 content categories:

1. Drugs
2. Gambling
3. Gambling Related
4. Gruesome Content
5. Hate Speech
6. Hacking
7. Malicious Sites
8. Nudity
9. Profanity
10. Pornography
11. School Cheating Information
12. Spam
13. Tobacco

---

20 Official Gazette of the Republic of Croatia nos. 167/2003, 79/2007, 80/2011, 125/2011, 141/2013 and 127/2014.

21 Official Gazette of the Republic of Croatia nos. 173/2003, 87/2005, 76/07, 30/2009, 128/2010, 49/2011 and 76/2013.

22 Official Gazette of the Republic of Croatia nos. 173/2003, 54/2005, 76/2007, 30/2009 and 49/2011.

23 Official Gazette of the Republic of Croatia nos. 173/2003, 54/2005, 76/2007, 30/2009 and 49/2011.

24 Official Gazette of the Republic of Croatia no. 112/12.

25 Official Gazette of the Republic of Croatia nos. 73/2008, 90/2011, 133/2012, 80/2013 and 71/2014.

26 The decision is not available, but the information on it is published on the CARNet web page: http://www.carnet.hr/filtriranje_sadrzaja (last visited on 1 August 2015).

27 See http://www.carnet.hr/en, last visited on 1 August 2015.

14.Violence.

This Decision is aimed at disabling such content when using school computers, regardless of the type of connection. It is said to be necessary due to the diverse content on the Internet, which is inappropriate or even damaging to the personalities of children given their age and level of maturity. The traffic filtering system operates by prohibiting display of the Internet pages in a certain category.[28] Each page is categorised on the basis of its content, while traffic is filtered by choosing the categories not to be displayed. CARNet is continuously categorising the pages and new database versions are automatically updated every couple of hours. In addition, it is possible to manually permit or prohibit a display of a particular page.

In relation to the higher education institutions who are members of the CARNet,[29] the filtering service against immoral content may be activated on an optional basis on all or only some of the computers in the institution. The system is the same as the one for the primary and secondary schools and there is a list of about 60 possible content categories available for a particular institution.[30] Among them there are some categories which at first glance might seem very restrictive, such as filtering the content to exclude display of search engines, but it might be justified with respect to some computers which are for instance used for taking the exams or alike. The system only filters the content on the web pages, i.e. the traffic using the HTTP protocol. The service does not enable filtering other types of traffic, such as e-mail, HTTPS traffic, FTP traffic, messages in news groups, P2P protocols (torrent, e-mule), instant messages (ICQ, MSN) and others. In order for a higher education institution to use this filtering service, the institution has to have a Proxy server which will redirect the desired HTTP traffic to the CARNet filtering system.

2.1.2. Blocking and filtering in the context of criminal proceedings

Under criminal law, there is no measure specifically and explicitly aimed at blocking and filtering an illegal Internet content. Accordingly, the two cases of which the author is aware which relate to some aspects of the matter, do not feature any official decision on blocking or filtering.

Homeland War Veterans Register case

The case which might have been relevant for the discussion under the blocking heading, but turned out to be of little assistance in understanding whether such blocking measure would be at all possible under the Croatian legal framework, was the unauthorised publication on 6 April 2010 of the registry of Croatian war veterans who participated in the Homeland Defence War in the period of 1991-1995. The content of the Homeland War Veterans Register was kept secret by the government and calls for its publication were regularly made because of suspicion that some of the persons listed therein were not actually war veterans. Eventually, the Register (or a part of it, as some claimed) was published on the Internet website www.registarbranitelja.com by an unknown person using a hosting company incorporated in the United States with the server based there as well. It could not have been browsed, but could have been searched by the veteran's name and surname and the military unit.

---

28 The system is called CA eTrust Secure Content Manager.

29 This includes, of course, all state universities and other state higher institutions.

30 The entire list of these categories is included in the application for filtering service downloadable through http://www.carnet.hr/filtriranje_sadrzaja/za_visokoskolske_ustanove (last visited on 1 August 2015).

The publication was not approved by the government and violated several laws, including the Data Secrecy Act and possibly the Personal Data Protection Act,[31] and as such represented a criminal offence under Article 133 of the Criminal Act. Under Article 25 of the Data Secrecy Act, the owner of the data may take any measure necessary to eliminate potential harmful consequences in case the data is destroyed, passed on or made available to unauthorised persons. Besides the Data Secrecy Act, there are the Rules on the Secrecy of Defence Data[32] as well as the Rules on Protection of Defence Data Secrecy.[33] Article 50 of the latter Rules provides that in the procedure following the misappropriation or disclosing of the secret data, the Security-Information Service shall establish among other things the measures necessary for eliminating possible harmful consequences of misappropriation or disclosing the secret data, and as well as the need to instigate criminal or military-disciplinary proceedings against the person whose acts brought about misappropriation or disclosing of the secret data. As a matter of fact, criminal charges against an unknown person were filed at the State Attorney's Office, but an indictment was never issued.

Soon after the publication, users started complaining that the Registry could not be accessed. It is not certain whether the Croatian authorities, including the State Attorney's Office, requested the US hosting company InvisiHosting to block access to the page from the Croatian IP addresses, or to take-down the page from the Internet or remove illegal content, or even to disclose the information about the person who is using their services. In any case, the response would probably have been negative.[34] At some point, the impossibility of accessing the website in question from Croatian IP addresses was reported. However, the US hosting company seems to have blocked the access to the Croatian users only because its server was overloaded and could not sustain such volume of traffic, and only until additional funds were collected to activate a hosting plan with larger bandwidth (or rather data traffic).[35] There were some reports in the media that the Croatian authorities had blocked the access to the internet site www.registarbranitelja.com to all IP addresses located in Croatia through the Croatian-based providers of internet access. Nonetheless, this was repeatedly denied by the internet service providers and there was no decision by any Croatian authority to that effect available to the public. Some say that pointing to providers was a result of the misinterpretation of the fact that the access to the site in question was blocked by the US hosting company to all Croatian IP addresses for the reasons mentioned above.

Komandir Šamil case

In the case colloquially called *Komandir Šamil*, the County Court in Split convicted a person of the criminal offence "public incitement to terrorism" under Article 97 of the Criminal Act. His offence consisted in a recorded speech calling for further military activities of resistance in Croatia, which was posted on You Tube. The speech occurred in the midst of a series of (probably) not related incidents in January 2013, in which several persons activated explosive devices in Zagreb. Although

31 For a discussion on whether this should be characterised as a violation of the Personal Data Protection Act see A. Musa/M. Jurić/M. Mataija, Transparency and Data Protection in the Context of E-Government: The Croatian Case, in: J. A. G. M. van Dijk/N. Jožanc (eds.), Information Society and Globalisation. Transformation of Politics, CPI/PSRC, Zagreb, 2011, pp. 175-207.

32 Official Gazette of the Republic of Croatia no. 39/2008.

33 Official Gazette of the Republic of Croatia nos. 112/1997, 79/2007 and 39/2008.

34 Vlasnik američkog servera za Index: Nismo Scotland Yardu odavali podatke, nećemo niti Hrvatima, Index.hr, 7.4.2010., http://www.index.hr/vijesti/clanak/vlasnik-americkog-servera-za-index-ako-nismo-scotland-yardu-odavali-podatke-necemo-niti-hrvatima-/484795.aspx (last visited on 28 July 2015).

35 See http://www.invisihosting.com/registar/ (last visited on 28 July 2015).

this was a crime related to terrorism, the speech posted on You Tube is still available for viewing from Croatia.[36] The only measure that was taken in this context was against the offender himself. Pursuant to article 75 of the Criminal Act, "**protective measure prohibiting Internet access**" was imposed, based on which this person no longer has access to Internet.[37] The measure is enforced by the **Croatian Regulatory Authority for Network Industries.**[38]

2.1.3. Blocking and filtering in the context of civil proceedings

If liability concerns the cases falling under the general rules in the Obligations Act, such as the **violation of personality rights**, the courts may order, *inter alia*, a condemnatory remedy – the claim **to remove the threat of damage**, intended to prevent the damage which has not yet occurred as well as to **stop the acts/omissions which would cause damage in the future**.[39]

General remedies also include the **preliminary measures available under the Enforcement Act**. For **securing pecuniary claims**, a court may order any preliminary measure which achieves the purpose of such security, and in particular it may: prohibit the opposing party from disposing of or from encumbering movables, seize those movables and place them into care of the proposing party or of a third person; seize and deposit cash, securities and similar objects with the court or a public notary. For **securing non-pecuniary claims**, a court may order any preliminary measure which achieves the purpose of such security, and in particular it may: prohibit the disposal and encumbrance of movables to which the claim is directed, seize them and place them into care of the proposing party or a third party, prohibit the disposal and encumbrance of rights to which the claim is directed and place those rights under management of a third party; prohibit the opposing party from taking actions which could cause damage to the proposing party and prohibit changes to things to which the claim is directed; order the opposing party to take certain actions necessary to preserve movables or the immovable property or to maintain the present state of things. Both these **provisions are open-ended** and the enumerated measures are only some of the most frequent ones. Therefore, although to the author's knowledge this has not yet been tested, **it should be possible for the applicant to ask, and for the court to grant, a measure ordering blocking or filtering an illegal Internet content**. An important condition for this would be to **make sure that the preliminary measure** consisting of blocking/filtering Internet content is suitable for, i.e. **achieves the purpose of securing the claim in question.**[40] Thus, the preliminary measure could be ordered in the proceedings between the person whose rights have allegedly been violated and the person who allegedly violated these rights, and is carried out by the third person – the provider of an Internet service (i.e. Internet access provider) who is ordered to block/filter the Internet content in question. Although the measure of taking down the content is more efficient,[41] when **the hosting provider and the servers are located abroad**, the blocking/filtering might be the only available measure left.

---

36 See https://www.youtube.com/watch?v=ITKXRlY2YOU (last visited on 1 August 2015).

37 This measure may be ordered against a person who has committed a criminal offence by means of the Internet whenever there is a risk that this person will commit the criminal offence again by misusing the Internet. This measure is intended to entirely unable that person to access the Internet.

38 See infra chapter 3. Procedural aspects. The Croatian Regulatory Authority for Network Industries which immediately upon receiving the court order has to inform all internet access service providers not to conclude a contract on Internet access with that person or to cease provision of such services to that person for the period in which the measure is in effect (and terminate subscription contract). See the Regulation on the Enforcement of the Protective Measure Prohibiting Internet Access, Official Gazette of the Republic of Croatia no. 34/2013.

39 Article 1047 of the Obligations Act.

40 See in general G. Mihelčić, Komentar Ovršnog zakona, Ogranizator, Zagreb, 2015, pp. 1025-1026 and 1040-1041.

41 See 2.2.

A person asking the court to order a preliminary measure related to pecuniary claim has to prove: a) the likelihood that the claim exists, and b) the risk that in the absence of such measures the other party will prevent or make it significantly more difficult to collect on a claim by transferring, hiding or otherwise disposing of her property. A person asking the court to order a preliminary measure related to non-pecuniary claim has to prove: a) the likelihood that the claim exists, and b) the risk that in the absence of such measures the other party will prevent or make it significantly more difficult to collect on a claim by altering the present state of the matter, or the likelihood that the measure is necessary to prevent violence or occurrence of irreparable harm.[42] However, the court may dispense with these conditions provided the person seeking the provisional measure provides a guarantee to indemnify against any damage that might be suffered by the other party.[43]

2.2. Take-down/removal of illegal Internet content

In Croatia there is **specific legislation in certain legal areas** which regulates taking down and/or removing illegal Internet content.

2.2.1. Take-down measures in the context of criminal proceedings

In cases where there are "bases for a doubt" that a person has committed a criminal offence that is prosecuted *ex officio*, **the police have the right and duty to take necessary measures** to find the perpetrator, to prevent the perpetrator from hiding or running away, to discover and preserve traces of the criminal offence and objects which might serve in establishing the facts and to collect all information which might be useful **for successful criminal proceedings.**[44] This seems to provide a wide basis for police action. However, the police services are usually careful not to act without a **court warrant** since the question of "bases of a doubt" may be invoked in the criminal proceedings and affect the validity of the evidence thus collected.[45] Besides, the police have to notify the State Attorney's Office immediately and not later than 24 hours after the measure has been taken.

Additionally, **the police** have the right to take certain measures even **before the commencement of the criminal proceedings** for the criminal offences punishable by no less than 5 years imprisonment, **if there is a danger in delaying the measure**. Such measures include **search** (Article 246) and **temporary seizing of an object** (Article 261). The police have to immediately notify the State Attorney of the search thus carried out, while in the case of the seizure of an object, the police have to notify the State Attorney of the results of the seizure.[46]

In the context of pre-trial proceedings, **the State-Attorney may make requests** the police, the Ministry of Finance, the State Auditing Office and other state bodies, organisation, banks and **other legal persons to submit certain data**, **provided that data is not confidential** under the law. The State Attorney may request these entities to control the business operations of a legal or natural person, **to temporary seize certain objects and documentation** in accordance with applicable law, **to perform surveillance** and to submit data which may serve as proof of a criminal offence or property acquired by committing a criminal offence, as well as **to request information on collected, processed and stored data** related to unusual and suspicious money transaction[47].

---

42 Article 346(1) of the Enforcement Act.

43 Article 349 of the Enforcement Act.

44 Article 207 of the Criminal Procedure Act.

45 The basis for rejecting the illegally obtained evidence in the criminal proceedings is, inter alia, in Article 250 of the Criminal Procedure Act.

46 Article 212 of the Criminal Procedure Act.

47 Article 206g of the Criminal Procedure Act.

Implementing the provisions of the Convention on Cybercrime, the Croatian Criminal Procedure Act provides for certain measures that authorities may take in order to assure **expedited preservation of stored computer data**, including traffic data.[48] This is included in the search of a moveable object under Article 257 of the Criminal Procedure Act. Such search includes a **search of the computer** and with it connected devices, other devices which serve for collecting, storing or transmitting data by telephone, computer or other communications, and of the data carrier. The basic rule is that the search may be conducted **only upon obtaining the court order**. Upon request of the State Attorney, the investigative judge or the trial judge (depending on the stage of the criminal proceedings) will decide on issuing a search warrant, which has to be **in writing and reasoned.**[49] The search is then carried out by the police or the investigator, seldom by the State Attorney. The authority performing the search has to hand over the warrant to the respective person, except in special circumstances, including if there is suspicion that this would enable hiding, destroying or damaging the object of search.[50] Upon the request of the authority performing the search, the person using the computer or having access to the computer or another device or data carrier, as well as the telecommunication service provider are under a duty to enable uninterrupted access to the computer, device or data carrier, and provide necessary information for uninterrupted use and realisation of the purpose of the search. Likewise, these persons are under a duty to immediately take the measures to prevent the data from being destroyed or changed. These measures may also be taken by the expert assistant to the authority conducting the search. Refusal to act according to these duties, without a just reason, may result in punishment by the investigative judge.[51] A search of an object itself does not result directly in the removal/taking down the content from the Internet, but is usually related to it, and often combined with the below mentioned measure of temporary seizure of an object.

The provision of Article 261 (rule) and 262 (exceptions) of the Criminal Procedure Act which relate to **temporary seizure of an object** may be pertinent to the issue of removal/taking down illegal Internet content. This is because, despite not being formally a measure for taking down or removing an illegal internet content, in practical terms, it has the same effect: **By seizing the server** (which is an object in the sense of Article 261 of the Criminal Procedure Act) on which the illegal Internet content is stored, **the content is effectively removed from the Internet**. This measure will, of course, be appropriate in **situations in which the server in question is located in Croatia**. An object may be seized if permitted under the Criminal Act or if it may serve to determine the facts in the proceedings. Persons in possession of these objects have a duty to hand them over,[52] and may be punished by an investigative judge if they refuse to do so without a just reason. Pursuant to Article 263 of the Criminal Procedure Act, the rules on seizure of an object apply also to **data stored in the computers** and with it connected devices, and devices which serve for collecting or transmitting data, data carriers and subscription information held by internet service providers. At the request of the State Attorney and within the time stated in the request, such data has to be handed over to the State Attorney in their entirety, in the original, legible and understandable form. Non-compliance is punishable. It is also provided that "data have to be stored in real time by the authority taking the

---

48 Article 331 states that the electronic evidence is gathered relying on the provisions of Articles 257, 262 and 263.

49 Article 242 of the Criminal Procedure Act. Exceptionally, where the delay related to obtaining the warrant would compromise the purpose of search, the State Attorney may himself/herself order the search of a person or search of a transport vehicle if there is suspicion that one of the enumerated criminal offences has been committed, including espionage or offences committed by the criminal organisation. See Article 245 of the Criminal Procedure Act.

50 Articles 243 and 244 of the Criminal Procedure Act.

51 Pursuant to Article 259, these persons may be fined up to the amount of HRK50.000,00, and if they still refuse to comply with the request may be imprisoned for as long as they do not comply, no longer than one month.

52 This duty does not oblige the accused person or persons who do not have a duty to testify.

measure."[53] In collecting, storing, protecting and keeping the data, the authority has to be mindful of the laws related to secrecy of certain data. In the circumstances, the data which does not relate to the criminal offence which is the reason for taking the measure and is needed by the person subject to the measure, may be recorded and stored and the data returned to that person before the proceedings are completed. The computer data seized may be kept by the authority based on the investigative judge's decree[54] as long as necessary, but no longer than six months. Upon expiration of this period, the data shall be returned, except where it is related to the criminal offences against computer systems, programmes and data (Title XXV of the Criminal Act), or where it is related to committing another criminal offence which is persecuted *ex officio* or where it serves as evidence of a criminal offence for which the procedure is ongoing.

According to the provision of Article 79 of the Criminal Act and Article 556 of the Criminal Procedure Act, **an object may be permanently seized provided it was intended or used for committing the crime**, **or its seizure is necessary for the protection of general safety, public policy or morals**. Permanent seizure is possible even if the person who committed an unlawful act is not convicted of a criminal offence. Such objects become property of the Republic of Croatia, except where the owner was not the one who committed the offence. Such owners have the right to claim return of the object or compensation of its market value unless he or she contributed (in gross negligence) to the commitment of the offence or got the object knowing of the circumstances which are the basis for its seizure. The court may order destruction of the permanently seized object.

2.2.2. Take down measures in the context of civil proceedings

If liability concerns the cases falling under the general rules in the Obligations Act, such as the **violation of personality rights**, the courts may order, *inter alia*, a condemnatory remedy – the claim **to remove the threat of damage**, intended to prevent the damage which has not yet occurred as well as to **stop the acts/omissions which would cause damage in the future**.[55]

General remedies also include the **preliminary measures available under the Enforcement Act:**[56] those for securing pecuniary claims and those for securing non-pecuniary claims. These are both open-ended provisions and the enumerated measures are only some of the most frequent ones. Therefore, although, to the author's knowledge, this has not been tested yet, it should be possible for the applicant to ask and for the court to grant a measure ordering taking down or removing an illegal Internet content. An important condition for this would be to make sure that the preliminary measure consisting in removing Internet content is suitable for, i.e. achieves the purpose of, securing the claim in question.[57] Thus, the preliminary measure could be ordered in the proceedings between the person whose rights have allegedly been violated and the person who allegedly violated these rights, and is carried out by the third person – the provider of an Internet service (i.e. the hosting provider) who is ordered to take down the content in question from the Internet. This will of course be efficient **if the hosting provider is located in Croatia**.

2.2.3. Intellectual property rights enforcement

---

53 This is literal translation of the provision, which in Croatian is somewhat difficult to understand, but the author's guess would be that it is meant to implement the provision of Article 20 of the Convention on Cybercrime.

54 The decree may be appealed.

55 Article 1047 of the Obligations Act.

56 The preconditions for ordering a preliminary measures are listed in 2.1.3.

57 See in general G. Mihelčić, Komentar Ovršnog zakona, Ogranizator, Zagreb, 2015, pp. 1025-1026 and 1040-1041.

Croatian law related to the protection of intellectual property rights contains several provisions allowing **remedies against Internet service providers independently of them being secondarily liable** or not. The Copyright and Related Rights Act in Article 185(1) states that the court can order **any preliminary injunction against the intermediary**, whose services are used by third parties to infringe the rights protected by the Copyright and Related Rights Act, with the aim of stopping or preventing the infringement. The court can grant such remedy at the request of the rights holder, provided that the latter shows the likeliness that her or his rights are being infringed or that there is threat of infringement. Such preliminary injunction can be granted *ex parte* if the rights holder shows the likelihood that the injunction would otherwise be ineffective or that irreparable harm would occur. Additionally, such preliminary injunction can be granted even if the rights holder has not yet filed a lawsuit against the infringer. However, in that case, in the decision granting the preliminary injunction, the court will order the rights holder to file the lawsuit within a fixed period of time to justify the preliminary injunction.[58] If the lawsuit was not filed at all or was filed with delay, the preliminary injunction will cease to produce effects. Other matters concerning the procedure for granting the preliminary measure are governed by the Enforcement Act.[59] Provisions identical to those in the Copyright and Related Rights Act are contained also in the Trademark Act,[60] the Industrial Design Act[61] and the Patent Act,[62] regarding the protection of trademarks, industrial designs and patents, respectively.

The Trademark Act, the Industrial Design Act and the Patent Act also contain provisions that allow the rights holder to file a lawsuit against the persons providing services used in acts infringing or threatening to infringe the protected right.[63] The plaintiff may ask the court, *inter alia*, to **order the service provider to stop the infringement and prohibit such or similar infringement in the future**,[64] **and to stop the act which is a serious threat of infringement as well as to prohibit the infringement by such an act**.[65] The courts decide upon these matters under the rules of civil procedure. When ordering remedies in litigation proceedings, Croatian courts tend to use general and descriptive language and usually avoid using technical terms. Therefore, although there is no specific case law related to the liability of information society service providers which would substantiate this, the author of this report is of the opinion that Croatian courts when deciding on a specific remedy against such a service provider might use very general language, such as ordering the service provider to "stop the infringement" or to "disable access to the illegal content", and not necessarily any technical language. Nevertheless, this order would include any (legally permissible) act necessary to comply with it.

2.2.4. Personal data protection laws

58 See Article 185(5) of the Copyright and Related Rights Act.

59 Official Gazette of the Republic of Croatia no. 112/2012. A person seeking the issuing of preliminary measures related to pecuniary claims has to prove: a) the likelihood that the claim exists, and b) the risk that in the absence of such measures the other party will prevent or make it significantly more difficult to collect on a claim by transferring, hiding or otherwise disposing of her property. However, the court may dispense with these conditions provided the person seeking the provisional measures provides a guarantee to indemnify any damage that might be suffered by the other party. See Article 344(1), Article 346(1) and Article 349 of the EA.

60 See Article 79b of the Trademark Act.

61 See Article 56d of the Industrial Design Act.

62 See Article 95j of the Patent Act.

63 See Article 76 of the Trademark Act, Article 54 of the IDA and Article 95c of the PA.

64 Article 76(2) and (4) of the Trademark Act, Article 54(2) and (4) of the Industrial Design Act and Article 95c(2) and (4) of the Patent Act.

65 Article 76(3) and (4) of the Trademark Act, Article 54(3) and (4) of the Industrial Design Act and Article 95c(3) and (4) of the Patent Act.

Any person believing that his or her right protected under the Personal Data Protection Act has been violated may ask the Personal Data Protection Agency to decide whether there was a violation or not.[66]

Report on the Property of Public Officials case

In the case related to publishing the "Report on the Property of Public Officials" on the Internet, the Agency established that there was a violation of the Personal Data Protection Act because of the excessive volume of information publicly made available. In its decree, the Agency prohibited the Committee for Deciding on the Conflict of Interest, which published the data on the Internet, from making it available on the Internet any longer as well as from "making it publicly accessible through the Internet search engines". The Committee was ordered to "erase the personal data […] from the Internet pages of the Committee", as well as to "take the appropriate technical protective measures in order to prevent browsing (sic!) the data by means of Internet search engines" and to give feedback to the Agency on the measures taken.[67] The last cited order by the Agency related to preventing "browsing" (they probably meant "searching") the data by means of Internet search engines is most probably related to an element in the webpage code whereby the web page administrator may disable crawling and indexing of the web page in question (the Robots Exclusion Protocol and/or Noindex Metatags Standard). Although these are sometimes called URL blocking methods, they are merely blocking the Internet search engines from including the web page in the search results, whereas the web page itself is not blocked and remains accessible for those who know it.

The Personal Data Protection Agency may also temporary prohibit processing of a certain data in the course of the proceedings and until the proceedings are over.[68]

2.2.5. Liability of internet service providers

The Electronic Commerce Act,[69] similar to Article 14 of the Directive on Electronic Commerce provides in Article 18, paragraph 1 that the provider of the service of storage of information shall not be liable for the information stored at the request of the recipient of the service subject to two conditions: 1) that the provider does not have the knowledge nor could have known of the illegal activity of the user or the contents of the stored data, as well as of the court proceedings related to claims for damages, which would arise from the illegal activity of the user or the contents of the stored data, and if he was not or could not have been acquainted with the facts or circumstances from which the illegal activity of the user would be apparent and 2) that **the provider, immediately upon obtaining the knowledge or becoming aware of the illegal activity or data, removes or disables access to the data**.

Furthermore, the Electronic Commerce Act, in its Article 19, contains another exemption to the liability of internet service providers for conduct of third parties using their services, which is not prescribed by the Directive. This exemption deals with hyperlinks and prescribes that the service provider which by means of electronic linking provides access to third party information is not liable for that information if it does not have the knowledge or could not have known of the illegal

66 Article 24 of the Personal Data Protection Act.

67 Personal Data Protection Agency, Class: UP/I-041-02/15-01/30, No. 567-02/01-15-01, 20 April 2015, http://www.azop.hr/news.aspx?newsID=387&pageID=249 (last visited on 29 July 2015).

68 Article 25 of the Personal Data Protection Act.

69 Article 1(2) of the Electronic Commerce Act sets out that the provisions of the Electronic Commerce Act shall not apply to the following: data protection, taxation, activities of public notaries, client representation and protection of their interests before courts, as well as games of chance with monetary stakes, including lottery games, casino games, betting games and games of chance on automatic machines.

activities of the user of the information and if it **immediately, upon obtaining knowledge or awareness of illegal activities or information, removes or disables access to the information**. As can be seen, the provision is very similar to, and it was modelled on, the safe harbour for hosting services. The main difference between the two provisions is that in the hyperlinks safe harbour, the illegality relates to the linked content and not to the hosted content.

To the knowledge of the author, the only case in which the safe harbour for hosting providers, or any safe harbour prescribed by the Electronic Commerce Act for that matter, was invoked before Croatian courts was the case in which a Croatian hosting provider was sued for damages by a university professor for an anonymous defamatory article posted on the then active Croatian blog platform MojBlog.com.[70] The defamatory article was, after its publication on the blog platform, picked up by a couple of very popular Croatian news portals and newspapers,[71] which are widely read in Croatia, and was allegedly, according to the claims of the plaintiff, read by tens of thousands of people. These follow-up articles specifically stated that the defamatory article was published on the blog platform MojBlog.com. The hosting provider, who was not aware of the disputed blog article prior to receiving the plaintiff's statement of claim (since the plaintiff contacted neither the owners of the blog platform nor the hosting provider with a request for removal of the article prior to initiating the court proceedings)**, immediately upon receiving the statement of claim and thus becoming aware of the defamatory article, removed the article in question from the blog platform**.[72]

In reply to the plaintiff's statement of claim, the hosting provider invoked Article 21 of the Electronic Commerce Act stating that hosting providers are under **no obligation to monitor** the information which they store or to seek facts or circumstances indicating illegal activity. Later in the proceedings, the hosting provider invoked the immunity prescribed by Article 18, paragraph 1 of the Electronic Commerce Act. Following these submissions, the plaintiff withdrew his claim against the hosting provider and the dispute ended without the court deciding on the merits.

Croatian law does not set out a "notice and take-down" procedure. To the knowledge of the author of this report, **the practice among Croatian hosting providers greatly varies** when they receive a request to remove or disable access to the allegedly illegal data, which came from the supposed rights holder and not an official state authority such as a court. Among the largest five or six hosting providers, at least two regularly refuse to remove any content without a court decision, while one has been known to react on a case-by-case basis assessing whether it is likely that the court would find the reported activities or data illegal and deciding whether or not to remove or disable access to the data based on its own assessment.

These differing reactions on the part of hosting providers might be the result of the current law in which there is an obligation on Croatian hosting providers to remove or disable access to the data immediately upon obtaining the knowledge or becoming aware of the illegal activity or data, but at the same time there is a lack of any judicial practice to clarify what is a sufficient takedown request, what is "knowledge of the illegal character of the internet content" or what would be the proper course of action for hosting providers when they receive such takedown request.

Finally, Article 20 of the Electronic Commerce Act prescribes that the provisions of the Act, particularly those pertaining to the liability of intermediary service providers, shall not affect the authority of courts and other competent bodies of the Republic of Croatia to order the information

---

70 Municipal Court in Zagreb, Pn-4423/06.

71 For example, Index.hr.

72 Interestingly, the owner of the blog platform was never sued by the plaintiff, even though its identity was very well known to the plaintiff.

society service providers and their users, at the request of the authorized person and in accordance with Croatian laws, **to eliminate or prevent infringements of law and regulations in force, and take other measures against them prescribed by law**. Therefore, the possibility of remedies being awarded against service providers to help restrain wrongful conduct by others independent of the service providers being secondary liable is explicitly allowed by the Electronic Commerce Act and the primary purpose of allowing such remedies prescribed by the Electronic Commerce Act is to eliminate or prevent infringements of the law.

3. Procedural Aspects

Based on the above, it may be concluded that the Croatian bodies competent for deciding on the limited instances of blocking, filtering or take-down or removing of illegal Internet content are **mainly the judicial bodies, but also the administrative bodies**.

When it comes to the **judiciary**, this includes criminal courts (pre-trial judge and criminal court judge/chamber of judges) and civil law courts (general jurisdiction courts and commercial courts). In all situations there is at least possibility of review by a higher court, and often also a possibility to have the case reviewed by the Supreme Court as well.

Particularly in criminal cases, there is a consistent *ex officio* court control of the legality of evidence. Thus, in the course of the pre-trial proceedings, the investigative judge has an *ex officio* duty to remove from the file all evidence which has not been legally obtained. If the investigative judge fails to do this, at the stage of controlling the indictment, the indictment judge is likewise obliged to remove from the file any illegally obtained evidence.[73] Finally, the trial judge has the same duty in the course of the criminal trial. Besides, the affected person (suspected, indicted or persecuted of the criminal offence) may appeal against any of the decisions on obtaining the evidence, and the appeal is decided by a judge (which judge will decide depends on the state of the proceedings). Additionally, there are certain special provisions guaranteeing the rights of the persons who are subject to criminal measures. In cases in which a certain measure has been taken by the State Attorney, investigator, or police officers, there is a possibility of a court review of such measures. For instance, if the search has been conducted pursuant to Article 245 of the Criminal Procedure Act, on the basis of the State Attorney's order and without a court warrant, the State Attorney is obliged to notify the investigative judge immediately and not later than eight hours following the search. Within the next eight hours, the investigative judge shall issue a decree on the legality of the search.[74] Furthermore, if the police have carried out the search without a court warrant or the State Attorney's order, pursuant to Article 246, the police have a duty to immediately hand over all the related documents (search record and search report) to the State Attorney.[75] In cases of urgent measures to preserve evidence under Article 212 of the Criminal Procedure Act, the police have a duty to immediately inform the State Attorney thereof[76]. In both these situations, the State Attorney may on its own motion remove illegally obtained evidence from the file or on the basis of an appeal by the affected person.

When it comes to **administrative bodies**, it is important to note that these are limited and are mainly regulatory agencies independent from the Government; they are the Personal Data Protection Agency or, with respect to the measure of prohibiting someone to access the internet, the Croatian Regulatory Authority for Network Industries. In such instances, Article 19 of the **Croatian Constitution guarantees legality of individual decisions of governmental agencies as well as their judicial review**. Such review occurs before the administrative courts and the Supreme Court. There is

---

73 Article 86 of the Criminal Procedure Act.

74 Article 245(3) and (4) of the Criminal Procedure Act.

75 Article 246(5) of the Criminal Procedure Act.

76 Article 212(6) of the Criminal Procedure Act.

also an option of turning to the Croatian Constitutional Court in case one believes that an individual decision (by a judicial or administrative body) violated any of his or her constitutional rights and freedoms.[77]

4. General Monitoring of Internet

There is **no law or regulation in Croatia which provides for general monitoring** of Internet content.

According to Article 21 of the Electronic Commerce Act, **internet service providers are under no obligation to monitor the information which they store, transmit or make available or to seek facts or circumstances indicating illegal activity**. However, if the service provider becomes aware that there is reasonable doubt that a user is performing illegal activities by using the service or that the user of the service has provided illegal data, it has to immediately **inform the competent state authority** thereof.

In addition, as evidenced hereafter, internet service providers may be requested to exercise certain monitoring or surveillance activities under both the Republic of Croatia Security-Intelligence System Act and the Electronic Communications Act; this function is to be activated only under the circumstances demanding such surveillance.

4.1. Surveillance measures in the context of national security

The Republic of Croatia Security-Intelligence System Act is intended to **enable systemic collection, processing and assessment of data which are of relevance to national safety**, with the aim of discovering and preventing acts of individuals or groups aimed at fighting against the existence, independence, integrity and sovereignty of the Republic of Croatia, promoting violent change of state government organisations, jeopardising human rights and basic freedoms and the basis of the economic state system, and which are necessary to make the decisions relevant to realising national interests in the field of national security.[78] These tasks are entrusted to **two agencies**: the **Security-Intelligence Agency** and the **Military Security-intelligence Agency**.

This Act further states that all natural and legal persons who possess public telecommunication networks and offer telecommunication services and access services in the Republic of Croatia are under a **duty to provide and maintain, at their own expense, the function of secret surveillance over telecommunication services, activities and traffic** listed in Article 33(3)(1) of this Act, as well as of the communication cables leading to the Operative-Technical Centre. This function consists of technical equipment and program support integrated in the telecommunication systems of these persons.[79] The Act lists the **measures for secret gathering of data which are then to be handed over to the bodies competent to proceed further** in the matter as explained below.

---

77 The constitutional complaint may be submitted before the Constitutional Court pursuant to Articles 62-80 of the Constitutional Court Act, Official Gazette of the Republic of Croatia nos. 99/1999, 29/2002 and 49/2002.

78 Article 1 of the Republic of Croatia Security-Intelligence System Act.

79 Detailed provisions are in the Regulation on duties in the field of national security of the Republic of Croatia for the naturel and legal persons in telecommunications, Official Gazette of the Republic of Croatia nos. 64/2008 and 76/2013.

4.2. Surveillance measures in the context of operations of providers of electronic communication services

The Electronic Communication Act provides for various obligations for the providers of electronic communication services which might be relevant under the topic of this report. Namely, the notion of "providers of electronic communication services" encompasses the providers of Internet access services. Despite the invalidity of the Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the **retention of data** generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC[80] which this Act was designed to implement, the Croatian legislator failed to amend the national legal framework, hence the legal status of these provisions is unclear. Thus, Article 105 of the Act prohibits any malicious or disturbing calls or messages or **any false identity presentation**. In case the operator of the service receives its **client's written notification** in which the client shows that it was probable that he or she received such calls or messages, **the operator has to make a record and store the data** on the number from which the call was made or message was sent, date and time of the call or message. On the basis of this data, the operator shall determine the name and surname of the end user making the call or sending the message, and his or her address and seat. The operator has to keep this record and **deliver the information to the police**. Operators are also under duty to cooperate among them in order to track and discover such illegal activities, especially to exchange the abovementioned data on the end user making the call or sending the message.

In addition, according to Article 107a of the Electronic Communication Act, which deals with the enforcement of data protection and electronic communication safety, the **Personal Data Protection Agency** or other body competent for the protection of personal data may, within their competences, ***ex officio* or upon the party's request, prohibit further violations** of Articles 99-107 of the Electronic Communication Act. In order to do so, they **may request all data they consider necessary for establishing possible violations** under Articles 99-107 **or which they consider necessary for the purpose of surveillance and enforcement** of Articles 99-107.[81]

Moreover, under Article 108 of the of the Electronic Communication Act, operators of the public communication networks and publicly available electronic communication services as well as **natural and legal persons who install, use or make available for use electronic communication network or provide electronic communication services** on the territory of the Republic of Croatia (regardless whether they are established in Croatia or another EU Member State) **have to provide and maintain, at their own expense, the function of permanent surveillance over electronic communication networks and services**, as well as electronic communication cables to the operative-technical body competent to activate and manage the measure of secret surveillance over electronic communications, in accordance with the special act regulating national security. This operative–technical body is competent to decide on the measures and standards of information security in relation to duties of the operators to provide and maintain functions of secret surveillance. Together

---

80 Official Journal L 105/54, 13.4.2006. Invalidity of the Directive is the result of the decision of the Court of Justice of the European Union on 8 April 2014: CJEU, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, joined cases C-293/12 and C-594/12, ECLI:EU:C:2014:238, 8 April 2014, available at: www.curia.europa.eu (last visited on 1 August 2015).

81 Articles 99-107 of the Electronic Communication Act relate to the following: integrity and security of electronic communication networks and services, violation of data protection in electronic communication, secrecy (or rather privacy) of electronic communications, secrecy of radio communications, deleting traffic data, display and hiding of the number from which the call is made, location data (without traffic data).

with the bodies competent to implement measures of secret surveillance, this body also controls the implementation of the measures and standards of information security. Duties of the operators towards the competent body to activate and manage the measures and the competent body to implement these measures are defined in special acts, related to national security and criminal procedure.

Such obligations are not subject to Articles 99-104 of the Electronic Communication Act or the special rules on personal data protection. Operators have to keep the list of their end-users, containing all data necessary for simple straightforward and momentary identification, which they must hand over to the competent bodies to implement the measures at their request. They must also hand over the traffic data on condensed or encrypted electronic communication. At the request of the competent bodies to implement the measures, the operators have to edisable users in using encryption functions or enable the bodies to remove encryption to facilitate secret surveillance over the electronic communication network and services.

At the request of the body competent to activate and manage the measure, the Croatian Regulatory Authority for Network Industries[82] shall inspect whether operators comply with the above duties.

Article 109 provides for the **data retention, obliging the operators of public communication networks and publicly available electronic communication services to retain data on electronic communication** referred to in Article 110 i**n order to enable investigation, discovering and criminal prosecution of the criminal offences** in accordance with the regulations in the field of criminal procedure, defence and national security. The period of retention is 12 months since the day of the communication in question.
Operators are under duty to comply with the following principles of safety of the retained data:

1. retained data has to be of the same quality and under the same safety and protection measures as data in the operator's electronic communication network,
2. retained data has to be adequately protected from accidental or illegal destruction, loss or change, unauthorised or illegal storage, processing, access or disclosure,
3. access to retained data has to be limited to the police officers and persons from the competent body to activate and manage the surveillance measure,
4. retained data has to be destroyed upon expiry of the retention period, except for data which was processed and stored for the purpose of use by the police officers and agents of the body competent to activate and manage the surveillance measure.

It is the operator's duty to ensure all technical and organisations measures and procedures to comply with these safety principles. They also have to report to the body competent to activate and manage the measure, about the procedures, number of requests, legal basis of the requests and type of data handed over. Control over the compliance with the safety principles, statistical data and annual reporting to the Commission is matter regulated in the by-law.

According to Article 110 of the Electronic Communication Act, the type of retained data include: data necessary to track down and determine the source of communication, data necessary to determine the destination of the communication, data necessary to determine the date, time and duration of the communication, data necessary to determine the type of communication, data necessary to determine users communication equipment or equipment considered as such, data necessary to determine the location of the portable communication equipment. This also includes unsuccessful

[82] Hrvatska regulatorna agencija za mrežne djelatnosti, http://www.hakom.hr/default.aspx?id=2628 (last visited on 1 August 2015), is generally competent to control the compliance of operators' activities with the Electronic Communication Act and related EU legal instruments, pursuant to its Article 111.

calls, but not calls that were never made. Retention of data which reveal the content of the communication is prohibited.

Non-compliance with the retention duties is punishable by fine.[83]

4.3. Surveillance measures by State inspection authorities

It is important to emphasize that not only courts, but also other competent bodies of the Republic of Croatia can act against internet service providers to help restrain wrongful conduct. This is for instance the case of the inspectors under the State Inspectorate Act. The main task of the **inspectors** is to **monitor the application of laws and other regulations in many areas**, amongst others, in the areas of trade, provision of services, consumer protection and protection of intellectual property rights. In carrying out the inspection tasks, the inspectors are authorized to inspect the business premises, equipment, business books, registries, documents, contracts and other business documentation which provides insight into the business activities of the inspected person.[84] They are also **authorized to temporarily seize the documentation and objects which can be used as evidence in misdemeanour proceedings or criminal proceedings.**[85] Persons being inspected must allow the inspector to perform the inspection and provide accurate information under the threat of a substantial fine.[86] If the inspector considers that the inspection would not be as effective, he or she **might even choose not to inform the inspected person of the upcoming inspection**.[87] Inspectors do not have to present any formal authorization when performing the inspection, such as any warrant or court order – the authority is given to them by the State Inspectorate Act. As a rule, the inspectors initiate the inspection proceedings *ex officio* and in theory no complaint against the inspected person is a necessary precondition for that purpose,[88] although the latter is rather a rule in practice. The inspector can forward documentation, and reveal facts and data only to courts, state administration bodies conducting misdemeanour proceedings, and other state bodies at their reasoned written request, and exclusively for use in court and administrative proceedings within their respective jurisdiction.[89]

4.4. Surveillance measures in the context of criminal proceedings

Whenever criminal proceedings are underway, Article 332 of the Criminal Procedure Act provides that the investigative judge may order **special temporary measures aimed at collecting evidence**. Such order is issued in writing **upon reasoned request by the State Attorney**, provided that alternative measures are not possible or would be disproportionately difficult, against the person in relation to which there are **bases of doubt that he/she has committed one of the criminal offences listed** in Article 334[90] of the Criminal Procedure Act. These special measures, the effect of which is to restrict certain constitutional rights of the person concerned, include:

---

83 Article 119 of the Electronic Communication Act.

84 See Article 27 of the State Inspectorate Act.

85 See Article 34 of the State Inspectorate Act.

86 See Article 30 and 61 of the State Inspectorate Act.

87 See Article 28 of the State Inspectorate Act.

88 See Article 33 of the State Inspectorate Act.

89 See Article 33(3) of the State Inspectorate Act.

90 The list of offences in this Article is quite long. It includes: public incitement to terrorism, prostitution, violations of child's rights, unauthorised sale of drugs, all offences against computer systems, programs and data, as well as offences infringing intellectual property rights if committed by means of computer systems or networks.

1. **surveillance and technical recording of** the telephone conversations and other **communications at distance,**[91]
2. **interception, collection and recording of computer data**,
1. entry into the premises for the purpose of performing the surveillance and technical recording of the premises,
2. **secret surveillance of persons and technical recording of persons and objects**,
3. use of secret investigators and informants,
4. simulated sale and purchase of objects and simulated provision of bribe and simulated receipt of bribe,
5. providing simulated professional services and entering into simulated legal transactions,
6. surveillance over transport and delivery of objects of criminal offence.

Finally, one may refer to article 339a of the Criminal Procedure Act, which provides for verification of **whether telecommunication contact was made**. If the registered owner or a user of a telecommunication means is suspected to have committed a criminal offence listed in Article 334 of the Criminal Procedure Act or another criminal offence which is subject to imprisonment of more than 5 years, the police may, on the basis of the order by the investigative judge, and for the purpose of collecting evidence, through the Operative-Technical Centre for Telecommunication Surveillance, request the operator of the public telecommunication services: to check the identity, duration and frequency of communication with a specific electronic addresses, to determine the location of the communication device as well as the locations of the persons making the electronic communication, and of the device's identification sign. The same can be done in relation to the registered owner or a user of a telecommunication means, not himself a suspect but connected to such suspect.

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

In the assessment of the compliance of the national provisions with the case law of the European Court of Human Rights (ECtHR), it is important to note that many of the provisions cited above have been under the scrutiny of the highest national or supranational courts.

As previously mentioned, the **Directive 2006/24/EC** of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC has been **declared invalid** as contrary to the EU law by the Court of Justice of the European Union (CJEU)[92]. This opened a question as to its legal effect, and more importantly, of the effect of the national laws implementing it. Regardless of the CJEU judgment invalidating this Directive, the Croatian implementation law remained the same. As a result of the lack of action by the Croatian legislator after the 2014 CJEU judgment, the providers concerned, including the **Internet access providers**, **remain thus obliged to operate certain monitoring/surveillance activities** based on the law implementing the Directive 2006/24/EC. This situation has however brought a level of uncertainty in the obligations as to monitoring of providers. From the decision of the CJEU, it seems reasonable to conclude that such monitoring activities do not constitute restrictions to fundamental freedoms, including freedom of expression, that are proportionate to the interests protected by such measures. As a result, it appears reasonable to

---

91 The measures under 1. may be ordered also against persons in relation to which there are grounds for doubt that the transmission from or to the perpetrator of one of the messages is related to the offence, or if that perpetrator is using their telephone or other communication device connections, as well as against persons who are hiding the perpetrator or aiding him not to be discovered.

92 CJEU, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, joined cases C-293/12 and C-594/12, ECLI:EU:C:2014:238, 8 April 2014, available at: www.curia.europa.eu (last visited on 1 August 2015).

conclude that such monitoring duties appear **incompatible with the ECHR safeguards and the case law of the ECtHR**.

Another issue which might be of importance is activities of **private actors** who are engaged in removing internet content **without any official decision** to that effect. A case in point in Croatia is the Centre for Education and Prevention of Violence, a non-profit organisation which, *inter alia*, is engaged in removing Internet pages of inappropriate content. They claim to be partners with Ministry of Internal Affairs, other government agencies and several cities, but they act on the basis of private requests, such as where a school teacher drew their attention to a Facebook profile which targeted several hundred school girls in Croatia, Bosnia and Herzegovina and Serbia. The so-called TaskForce managed to remove the profile.[93] So far, there has been no debate over these activities, probably because they are particularly aimed at protecting children from Internet violence.
At the Croatian national level, it is important to cite Article 3 of the Constitution, which lists the highest values of the Croatian constitutional order, among which freedom, equal rights, respect for human rights and rule of law. Article 16 then provides: "Freedoms and rights may only be curtailed by law in order to protect the freedoms and rights of others, the legal order, and public morals and health. **Any restriction of freedoms or rights shall be proportionate to the nature of the need to do so in each individual case**." Article 35 guarantees respect for and legal protection of each person's private and family life, dignity, and reputation. Article 36 provides for the freedom and privacy of correspondence and all other forms of communication, and permits only for restrictions necessitated by the protection of national security and the conduct of criminal prosecution where prescribed by law. Article 37 focuses on the safety and secrecy of personal data and provides that without consent from the person concerned, personal data may be collected, processed and used only for the purpose there are collected and under the conditions specified by law. Protection of data and oversight of the operations of information systems in the state shall be regulated by law. Article 38 further guarantees the freedom of thought and expression, as well as access to information, and forbids censorship. Hence, whenever take down measures are ordered by civil courts, thus under review of an independent judge, they are deemed to be respectful of freedom of expression, as national laws and their application or interpretation by courts are subject to Articles 38 and 16 of the Constitution mentioned above. Any person who believes that his or her fundamental rights and freedoms have been violated by a decision of a court or another competent body in the Republic of Croatia, such as the one on measure of taking down an Internet content, may bring before the Constitutional Court a constitutional complaint – protection *in concreto.*[94]

However, the provisions mentioned above do not prevent constitution-based examinations of national law provisions. There is also a possibility to claim protection *in abstracto*. The request for an assessment of the constitutionality of an act (in force in Croatia) may be submitted to the Constitutional Court of the Republic of Croatia by the Government, the President of the Republic, the fifth of the Members of Parliament, the parliamentary committee, the Supreme Court, as well as any other court if such issue is raised before it.[95] In addition, every person may submit to the Constitutional Court of the Republic of Croatia the proposal for assessment of constitutionality of an act (in force in Croatia) with the Constitution.[96] In such cases where the Constitutional Court of the Republic of Croatia is called to *a posteriori* control the restrictions of human rights, it is relying on the basic principles as established and interpreted in the ECtHR case law, such as that restricting

---

93 Đakovački TaskForce uklonio Facebook profil koji je poticao na mržnju protiv tinejdžerki u tri države, Index.hr, 6.11.2014., available at: http://www.index.hr/vijesti/clanak/djakovacki-taskforce-uklonio-facebook-profil-koji-je-poticao-na-mrznju-protiv-tinejdzerki-u-tri-drzave/782202.aspx (last visited on 1 August 2015).

94 Article 62 of the Constitutional Court Act,

95 Article 35 of the Constitutional Court Act.

96 Article 38 of the Constitutional Court Act.

provisions have to be easily accessible and foreseeable,[97] that restrictions must be adopted in a view of legitimate goal and they must be proportionate to that goal and necessary in democratic society,[98] as well as that there must be safeguards as to arbitrariness and abuse of human rights in the form of a court review independent of intervention by administrative authorities.[99]

In its decision of 2012, the Constitutional Court of the Republic of Croatia exercised its right to **review the constitutionality of a number of provisions of the Criminal Procedure Act.**[100] It has done so not only on the basis of the Croatian Constitution, but also of the ECHR (including Articles 2, 3 6, 8 and 13 thereof) and its Protocols (Protocol 13), including extensive reliance on the ECtHR case law. Likewise, there are arguments based on comparative law. The Court has detected a large number of violations of both the Constitution and the European Convention on Human Rights (ECHR) and has invalidated nearly half of the Act. The Act was then thoroughly revised to comply with the Constitutional Court's objections and the Court has not acted since, although it has preserved the right to *ex officio* re-examine the constitutionality of the new provisions. In its findings, the Constitutional Court found violation of the following constitutional principles: principle of proportionality, principle of judicial review, principle of fair process, protection of personal freedoms, protection of personal and family life, home and correspondence and principle of legality in the criminal procedural law. The Court's decision produced various effects: *inter alia*, it made sure that the procedural guarantees and right to a defence in pre-trial proceedings are rules rather than exceptions; it ensured that there are only proportionate, clear and legitimate restrictions to human rights; it reinforced the role of the judge throughout the proceedings, and it redrafted certain provisions to achieve sufficient precision and predictability in application so as to leave no room for arbitrariness.[101]

In its decision, the Constitutional court addressed the constitutionality of the provisions of the above cited Articles 257(1); 262(1)(3) and (4), 262(2)(1) and 262(3), 262(4) and 262(5); 331(2) and 332(2), 332(4) and 332(1) and 332(7) and 334. In examining Article 332(2) of the Criminal Procedure Act, the Court found some of its aspects to be unconstitutional. This Article empowers the investigative judge to order special temporary measures aimed at collecting evidence. The invalidated text of this Article provided for 6 month-long measures, which could have been extended twice for six months, altogether lasting a year and a half. The Court found this to be an unjustly long period of time.

---

97 See e.g. Constitutional Court the Republic of Croatia, Decision U-I-241/1998 of 31 March 1999, Official Gazette of the Republic of Croatia, no. 38/1999; Constitutional Court of the Republic of Croatia, Decision U-I-448/2009, 19 July 2012, Official Gazette of the Republic of Croatia, no. 91/2012.

98 See e.g. Constitutional Court the Republic of Croatia, Decision U-I-241/1998 of 31 March 1999, Official Gazette of the Republic of Croatia, no. 38/1999; Constitutional Court the Republic of Croatia, Decision U-I-1156/1999 od 26 January 2000, Official Gazette of the Republic of Croatia, no. 14/2000; Constitutional Court the Republic of Croatia, Decision U-I-884/1997, U-I-920/1997, U-I-929/1997, U-I-956/1997, U-I-453/1998, U-I-149/1999 of 3 February 2000, Official Gazette of the Republic of Croatia, nos.20/2000 and 28/2000; Constitutional Court the Republic of Croatia, Decision U-I-236/1996, 3 May 2000, available at www.usud.hr (last visited on 22 September 2015); Constitutional Court the Republic of Croatia, Decision U-III-5917/2013, 23 May 2014, available at www.usud.hr (last visited on 22 September 2015).

99 Constitutional Court the Republic of Croatia, Decision U-III-1142/2013, 1 December 2014; Constitutional Court the Republic of Croatia, Decision U-III-5892/2011, 27 May 2015; Constitutional Court the Republic of Croatia, Decision U-III-3335/2012, 1 July 2015; Constitutional Court the Republic of Croatia, Decision U-III-6219/2013, 3 June 2015; Constitutional Court the Republic of Croatia, Decision U-III-1311/2014, 17 July 2015; Constitutional Court the Republic of Croatia, Decision U-III-1248/2012, 17 July 2015, all available at www.usud.hr (last visited on 22 September 2015).

100 Constitutional Court of the Republic of Croatia, Decision U-I-448/2009, 19 July 2012, Official Gazette of the Republic of Croatia, no. 91/2012.

101 Z. Đurđević: Odluka Ustavnog suda RH o suglasnosti Zakona o kaznenom postupku s Ustavom, Hrvatski ljetopis za kazneno pravo i praksu (Zagreb), Vol. 19, No. 2, 2012, pp. 409-438, especially p. 437.

Besides, the Court stated that the criteria for deciding on taking these measures ("important reasons" and "particular complexity of the case") are **not consistent and are insufficiently clear and precise, and, as such, unpredictable and left to the discretion of the investigative judge**. Therefore, these criteria, according to the Court, **cannot serve as basis for limiting the human right to privacy.**[102] In examining Article 334(4), the Court noted that imprecise phrasing was used when stating that special measures aimed at collecting evidence in Article 332(1) may be ordered in relation to, "criminal offences committed to the detriment of the children and minors". The Court explained that, although this provision has a legitimate aim in protecting children and youth (which is also the State's task under Article 61 of the Croatian Constitution), this phrasing is unconstitutional because it may relate to virtually any criminal offence where there is some relation to a child or a minor. On the other hand, the purpose of the catalogue of criminal offences in Article 334 is to limit the special measures in Article 332 (which restrict certain constitutional rights) exclusively to those criminal offences which present a very serious threat to society. Thus, **the provision of Article 334(4) was invalidated as contrary to the rule of law and legal certainty and foreseeability**. The provision of Article 334 as it stands now contains the catalogue of specific criminal offences from the Criminal Act, and no open-ended rule such as the one that was invalidated. It is therefore considered to be in compliance with the criteria set out by Article 10 of the ECHR and the Croatian Constitution.

After this recent evaluation of the Criminal Procedure Act by the Croatian Constitutional Court, the level of respect for human rights and fundamental freedoms in the Croatian criminal procedural law has been reinstituted. However, doctrine still questions some provisions, such as Article 75 of the Criminal Act called "protective measure prohibiting Internet access", which is seen as problematic in that it entails the absolute prohibition of Internet access to an offender in question and is thus disproportionately restrictive to the offender's human rights and potentially contrary to Article 10 of the ECHR.[103]

Submitted on 23 September 2015 by
Assist. Prof. Dr. Ivana Kunda

University of Rijeka

102 Para 170 of the Constitutional Court Decision U-I-448/2009.

103 D. Škrtić, Sigurnosna mjera – zabrana pristupa internetu, conference paper June 2013, 14. Slovenski dnevi varstvoslovja, www.fvv.um.si/dv2013/zbornik/informacijska_varnost/skrtic.pdf (last visited on I August 2015); L. Cvitanović/I. Glavić, Uz problematiku sigurnosne mjeere zabrane pristupa internetu, Hrvatski ljetopis za kazneno pravo i praksu (Zagreb), Vol. 19, No. 2, 2012, pp. 891-916.