LITHUANIA

Comments and remarks to the "Comparative study on blocking, filtering and take-down of illegal internet content" (Excerpt, pages 397-411), which was prepared on 20 December 2015 by the Swiss Institute of Comparative Law upon an invitation by the Secretary General of the Council of Europe

1. Legal Sources

Para 1, Sent 2: [...] issues related to take-down of illegal internet content **and blocking of internet services**.

Para 3, Point 2: **conventions** to be used instead of ~~agreements~~.

Para 3: Two additional laws to be added to the list of the main statutory and other legislative sources that permit or allow for the blocking, filtering and take-down of illegal internet content in the Lithuania:

- The Law on Cyber Security[1] that grants competent national authorities, namely the National Cyber Security Centre and the police, the right to give motivated orders to internet and hosting service providers to temporarily block internet access to a person whose infrastructure is involved in a cyber-incident or a crime. Police rights are further specified in an implementing act – Procedure on the Organization of Police Work in the area of Prevention and Investigation of the Cyber Incidents with Signs of a Crime[2], adopted by the Lithuanian Police Commissioner General. It should be noted that application of these legal acts to fight against "illegal content" (child pornography, infringements of intellectual property rights, incitement of terrorism and etc.) is possible if it is connected to cyber-incidents related to "pure cybercrime" (illegal access, illegal interception, data interference, system interference, etc.).
- The Criminal Procedure Code that sets out grounds and procedures for seizure, which may be used as a measure for blocking and removing unlawful online contents by way of seizing relevant infrastructure.
- The Gaming Law[3] that grants Gambling Supervisory Authority the right to give motivated orders to internet and hosting service providers to block access to the resources related to unlawful online gaming and to remove any related content.

2. Legal Framework

2.1. Blocking and/or filtering of illegal Internet content

General remark regarding the insights in Paras 2–6: As another consequence of a lack of comprehensive regulation in this area may rather be that the rights to block illegal online content are dispersed among several competent entities, including the police, courts (civil, administrative and criminal), and specific regulatory authorities (such as for instance Gaming Control Authority under the Ministry of Finance of the Republic of Lithuania[4]) within the limits of their competence. Therefore, claiming that illegal content may only be blocked or filtered only by way of civil law

---

[1] https://www.e-tar.lt/portal/lt/legalAct/5468a25089ef11e4a98a9f2247652cf4 // The Law on Cyber Security of the Republic of Lithuania (in force since 1 January, 2015)

[2] https://www.e-tar.lt/portal/lt/legalAct/c959d190ab8e11e48ebccd46991dfff9

[3] https://www.e-tar.lt/portal/lt/legalAct/TAR.E5509883EBB4/FVtQVAYKkH // The Gaming Law of the Republic of Lithuania, para. 1, Art. 20^7.

[4] http://www.lpt.lt/en/about-institution/

and civil procedure measures does not correspond current status. The study should include information about other measures as well:

- Criminal procedure provides for the possibility to use seizure as means of blocking (and removal of) illegal internet content. When there are grounds to believe that there are crime instrumentalities, crime proceeds or other objects and documents that might be of significance to an investigation, in a certain place or at disposal of a certain person, law enforcement (investigators or public prosecutors) may perform a search and seize any such objects or documents. By way of seizing infrastructure (servers) used to host illegal internet content, access to such content is blocked.

- the Law on Police provides police officers with general power to give lawful orders to a person not directly subordinate to him/her for the purposes of prevention and investigation of criminal offences and other law violations. Lawful orders of a police officer are obligatory to all natural and legal entities and must be executed immediately. It should be noted, that the mentioned provision of the law is not absolute or unlimited, because such orders of the police becomes obligatory when police rights specified in other national laws (Law on Criminal Intelligence, Code of Criminal Procedure, etc.) are implemented. This rule is applied also to police orders to block illegal internet content.

- The Law on Cyber Security grants the right to block the provision of internet or hosting services to a user whose infrastructure participates in a cyber-incident or a criminal offence. This right is granted to two entities – National Cyber Security Centre (NCSC) and the police.

  NCSC is a specialized entity responsible for cyber security of the state and critical infrastructure. Among other powers and responsibilities, during a cyber-incident, it has the right to give lawful orders to public entities responsible for managing state information resources and critical infrastructures. Also, it has the right to order internet and hosting service providers to temporarily (up to 48 hours) block user's access to the services.

  The police have similar right to order internet and hosting service providers to temporarily block (up to 48 hours without court sanction, over 48 hours with court sanction) provision of services to a user whose infrastructure participates in a cyber-incident that has signs of a criminal offence.

- Based on the provisions of the Gaming Law, the right to block access to the content in breach of the online gambling regulations is granted to the Gambling Regulatory Authority. If the GRA establishes in the course of an investigation that any natural or legal person illegally organizes online gambling, it can order internet or hosting service provider to block access to any resources and infrastructures related to such illegal gambling activity. Also, the GRA has the right to giver order to the providers to remove respective illegal content. Prior to giving such orders, the GRA must obtain permission of an administrative court.

2.2. Take-down/removal of illegal Internet content

Para 1 Sent 1: We suggest the following wording: **Even though there is also a lack of subject-specific regulation with respect to take-down/removal of illegal internet content, same or similar grounds and rules apply as to blocking and filtering.** Last sentence in Para 1 should be deleted.

Para 2 Sent 1: Suggested wording: **In addition to the provisions applicable to blocking and filtering as set out in Q.2.1 above, the Access Termination Procedure outlines** [...]

3. Procedural Aspects

Para 1 Sent 1&2: Suggested wording: **Authority to block, filter and take-down illegal internet content is dispersed among several authorities in Lithuania. Thus, such decisions are made by the judiciary, the police and specific regulatory authorities within the limits of their competence.**

4. General Monitoring of Internet

Para 1: Suggested wording: **In Lithuania, there are several entities that monitor internet content to the extent relevant to their scope of activity. These entities are the National Cyber Security Centre, CERTs, state security authorities, defence, the police and other law enforcement agencies, regulatory authorities. Also, certain monitoring activities and initiatives are implemented by the private sector, mainly by major internet and hosting service providers.**

Para 4: We suggest supplementing this paragraph with brief explanation that all incidents having the signs of a criminal offence noted while monitoring the Internet are forwarded for the attention of the police, which in its turn evaluates the information and decides upon the need to start an investigation.

***

Lilija Omeljančuk[5]

Žilvinas Sideravičius[6]

[5] The present Lithuania's national expert to the Cybercrime Convention Committee (*T-CY*) of the Council of Europe, since April, 2015.

[6] The former Lithuania's national expert to the Cybercrime Convention Committee (*T-CY*) of the Council of Europe, since June, 2010 till April, 2015)