JUDr. PhDr. Tomáš Gábriš, PhD., LLM, MA
Právnická fakulta
Univerzita Komenského
Šafárikovo námestie 6
810 00 Bratislava 1
Slovenská republika
tomas.gabris@flaw.uniba.sk

Graduated in law and history from the Comenius University in Bratislava and Trnava University in Trnava (Slovakia), Central European University in Budapest (Hungary), and Tilburg University in Tilburg (Netherlands). Attorney-at-law, licensed by the Slovak Bar Association. Since 2004 employed at the Faculty of Law of the Comenius University in Bratislava, currently as Assistant Professor, teaching a.o. courses on Cyber Law and Law and Technology.

Bc. Ladislav Kovár
Právnická fakulta
Univerzita Komenského
Šafárikovo námestie 6
810 00 Bratislava 1
Slovenská republika
ladislav.kovar@flaw.uniba.sk

Graduated as Bachelor of Law from the Comenius University in Bratislava (Slovakia). Paralegal/Assistant in the Law Office of Dr Tomáš Gábriš. Since 2003 employed as System Operator and Webmaster of the Faculty of Law, Comenius University in Bratislava.

RESTRAINING THE INFORMATION dissemination on the internet[1]

Tomáš GÁBRIŠ – Ladislav KOVÁR

ABSTRACT:
Restriction of information dissemination on the Internet has various facets and follows various goals. In general, in democracies, it is only allowed upon meeting the standards of balanced rights, freedoms and overriding interests – freedom of expression/speech on the one hand and the protection of rights and freedoms of other human beings or public interest on the other. Proportionality has to be always taken into account in order not to disproportionately affect (limit) fundamental rights. Besides governmental restrictions, private restriction of information dissemination is also present, performed by religious groups, both public and private mass media and private individuals and corporations. Two types of restrictions – technical and non-technical can be discerned. From another point of view, self-censorship, or internal restriction can also be distinguished as opposed to external restrictions. Finally, preventive and repressive restrictions are being applied.

KEYWORDS:
Internet, censorship, freedom of speech, freedom of expression, personality rights, self-censorship

Introduction

"I disapprove of what you say, but I will defend to the death your right to say it."
Voltaire

Restraining the information dissemination on the Internet - in the various forms that will be addressed in this paper - is often perceived as being a restriction of the freedom of speech or of the freedom of expression. For the sake of this paper, the expression is considered a broader notion than speech, involving also other than verbal expressions. In general, just like with other rights and freedoms, freedom of speech/expression is not unlimited. Everyday exploitation of the freedom of speech/expression in interpersonal relations, be it in oral, pictorial or written form, has to take into account its limits represented e.g. by the personality rights. Freedom of speech/expression may namely not be used to breach the right to human honour and dignity; at least that is the prevailing view within the European legal systems. Balancing the rights/freedoms seems to be the crucial point in their relationship and in its legal assessment by the European courts. The U.S. approach, on the other hand, is marked by a relative priority of the freedom of speech in relation to personality rights. However, not only personality rights can negatively be affected by (ab)using the freedom of speech. It can also be public interest, public order, or national security, which bring governments of the USA, China and other major nations to restrain the free dissemination of information.

1 The paper was written within the project „Cultural and religious differences, migration and human rights", no. 1/0507/12, financed by the VEGA Slovak Republic.

Restraining the information dissemination was usually considered a practice used by non-democratic regimes and was labelled as censorship.[2] In the history of Czechoslovakia, this was the case with the so-called communist regime (1948-1989), when a special Office for censorship was established.[3] Currently it is existing in countries such as China, Iran, Saudi Arabia, Tunis, Myanmar (Burma), North Korea, Uzbekistan and many others that apply censorship of the Internet, where the restraining of information dissemination takes a form of fighting against so-called cyber dissidents.[4]

Still, restraining the information dissemination on the Internet should be considered a broader notion than censorship of the Internet, as it also comprises restraining the information dissemination aimed at protecting the basic values such as human life, health and dignity, as well as the public order and public interest. Restraining the information dissemination is thus not only a mark of undemocratic regimes where this restraining is labelled as censorship, but may arise from democratic protection of rights of the others, public interests and thus it can be considered proportionate and reasonable. In general, restraining the information dissemination on the Internet may have various reasons and protect various interests:

1. Protection of personality/human rights (e.g. human dignity)
2. Protection of intellectual property rights/special personality rights
3. Political or security reasons (anti-terrorist policy or simple abuse of political power)
4. Economic/commercial reasons (e.g. protection of trade secrets).

As a consequence, striking a balance between the rights and interests of the various conflicting actors, i.e. the proportionality of restraining the information dissemination is a major legal problem. Additionally, the emergence of cyberspace brings various new challenges to this mutual balancing of the rights, freedoms and interests[5] – it is mainly the existence of social networks, blogs, and potential ubiquity of expressions and speeches that raise various issues[6] such as those of applicable law and of jurisdiction of courts.

1 Actors restraining the information dissemination on the internet

The main actors restricting the information dissemination on the Internet are the following ones:[7]

Governments

This happens mostly for the political and public policy reasons: either to protect the undemocratic regime and suppress cyber dissidents,[8] or in the strive to protect democracy against terrorist or other inimical attacks,[9] or further following the social and moral goals of so-called public order (e.g. in case of protection against child pornography). This kind of restrictions may be considered repressive, as opposed to preventive (auto-/self-) censorship.

2 The origin of the term comes from Roman Republic and later Roman Empire, where in the 5th Century BC the office of a censor was established with the task to assess the number of population and to acknowledge rights and obligations of citizens according to their assessed property (taxes, military service). Personal behaviour in private as well as in public was also assessed by the censors with a possible punishment, e.g. exclusion from the Senate.

3 ADAMOVÁ, Karolína: Cenzurní zásahy do české kultury v letech 1948-1989. In: Vývoj práva v Československu v letech 1945-1989. Ed. K. Malý, L. Soukup. Prague : Karolinum, 2004, p. 281-306.

4 Cf. „For Russians,the Internet is the 21st century version of samizdat—the material in cyberspace is there for everyone to read." CASO, Frank: Censorship. New York: Facts On File, 2008, p. 102-103.

5 GÁBRIŠ, Tomáš: Definícia veci a výzvy modernej vedy. In: Justičná revue, 60, 2008, pp. 529-40.

6 DRGONEC, Ján: Masmediálne právo na Slovensku v ére digitalizácie elektronických masmédií. In: Communication Today, 2, 2011, 2, pp. 20-33.

7 Cf. CASO, Frank: Censorship. New York: Facts On File, 2008, p. 14-15.

8 In China, both websites of those promoting free market economy as well as of leftists arguing against privatisation are censored: http://www.guardian.co.uk/world/2012/may/02/free-market-thinktank-website-shut-china (accessed 01 July 2013).

9 For an overview, consult a study by the Open Net Initiative at: http://www.guardian.co.uk/technology/datablog/2012/apr/16/internet-censorship-country-list (accessed 01 July 2013).

Taking an example of China, Section Five of the "Computer Information Network and Internet Security, Protection, and Management Regulations", approved by the State Council on 11 December 1997 officially states the following: No unit or individual may use the Internet to create, replicate, retrieve, or transmit the following kinds of information:

1. Inciting to resist or breaking the Constitution or laws or the implementation of administrative regulations;
2. Inciting to overthrow the government or the socialist system;
3. Inciting division of the country, harming national unification;
4. Inciting hatred or discrimination among nationalities or harming the unity of the nationalities;
5. Making false statements or distorting the truth, spreading rumours, destroying the public order;
6. Promoting feudal superstitions, sexually suggestive material, gambling, violence, murder;
7. Terrorism or inciting others to criminal activity; openly insulting other people or distorting the truth to slander people;
8. Injuring the reputation of state organizations;
9. Other activities against the Constitution, laws or administrative regulations.[10]

On the other hand, in the United States, state-mandated Internet filtering occurs on computers in public libraries and in schools, based on the Children's Internet Protection Act (CIPA). A law passed in December 2000 requires any library receiving certain forms of federal aid to install Web "blocking" programs that censor a wide range of online material.[11]

A specific situation "sui generis" is the restriction and repression aimed against those who reveal information that is considered sensitive and confidential due to reasons of public security and public interest – such as the cases of information disseminated in the Wikileaks and Edward Snowden campaigns.

Finally, in Europe, website content related to Nazism or Holocaust denial is usually blocked in many countries. In general, it is child pornography, hate speech, sites that encourage the infringement of intellectual property rights and infringing on confidential public security information that are being blocked in many countries throughout the world, including democracies.[12]

Religious groups

Religious groups intend to prevent their members to access information that may conflict with their dogmatic teaching. It may be mostly Muslim religious groups that censor websites and information on other religions.

Private individuals

Individuals censoring access to information are mostly parents trying to prevent their children from accessing websites and information considered by the parents as harmful to their children´s morals and integrity. There are various commercial products providing help with such a private censorship. The best known is the following software:

- Cyber Patrol™ Filtering Software
- Sites Blocked by Cyber Patrol
- CYBERsitter™ Filtering Software
- Bess Filtering Services
- CleanNet™
- McAfee Office (Guard Dog)
- American Family Association.

10 http://en.wikipedia.org/wiki/Internet_censorship_in_the_People%27s_Republic_of_China (accessed 01 July 2013).

11 http://www.aclu.org/technology-and-liberty/aclu-disappointed-ruling-internet-censorship-libraries-sees-limited-impact-ad (accessed 01 July 2013).

12 http://en.wikipedia.org/wiki/Internet_censorship (accessed 01 July 2013).

Another way how the individuals perform the information restrictions on the Internet might be self-restriction induced by a threat by a legal action against those who (at least allegedly) interfere with the protected rights and interests. This may either lead to a situation of forced auto-restriction in order to evade a potential lawsuit, or it may lead to a court proceedings which repressively forces the "publisher" (this need not be a newspapers corporation) to remove the information from the Internet.

Mass media

Mass media mostly exert preventive auto-censorship (self-restriction of information dissemination). The owner or the person in charge of the media may sometimes have a strong word in deciding which information to publish and which not, often depending on political orientation of the media/owner. The other type is the already mentioned auto-censorship under the threat of a lawsuit.

Corporations

Corporations providing information on the Internet exert preventive self-censorship (self-restriction) in a way similar to mass media and private persons. They present only information they consider relevant for their own benefits, additionally attempting to prevent potential lawsuits.

2 Methods of external restriction of the information dissemination on the internet

The methods of restricting information dissemination on the Internet might be distinguished as internal (preventive self-censorship under threat of legal actions or criminal prosecution) or external. The external restriction of information dissemination (including censorship) may take forms of non-technical restriction (e.g. lawsuits and repressive legal sanctions for publishing the information) and technical restriction, which is used mostly as prevention. External restriction can hence be both preventive and repressive.

Within the non-technical restriction, e.g. hotels in China advise Internet users to obey local Chinese Internet access rules by leaving a list of Internet rules and guidelines near the computers. These rules, among other things, forbid linking to politically unacceptable websites, and inform Internet users that if they do, they will have to face legal consequences.[13]

The currently most discussed dimensions of non-technical restrictions are on the other hand connected to the United States and their allies´ persecution of "spies" and "treason offenders" such as Bradley Manning, Edward Snowden or Julian Assange in the "Wikileaks-gate". These are instances of legal repercussions aimed against those revealing information considered sensitive and important for the national security and public order by the Western governments.

From the point of view of methodology of technical information restrictions, Internet filters may be used that work by blocking specific websites that are known to contain objectionable material; other systems use a list of banned words - if the requested webpage contains a banned word, the page is blocked. Others check the pages for embedded codes that indicate the page is not intended for children. Hence, blocking and filtering can be based on relatively static blacklists. Still, filtering may be determined more dynamically based on a real-time examination of the information being exchanged.[14] Some filtering companies use human employees in this respect in order to inspect webpages and make a judgment whether to block or not. A combination of these techniques may be used in practice as well.[15]

13 http://en.wikipedia.org/wiki/Internet_censorship_in_the_People%27s_Republic_of_China (accessed 01 July 2013).
14 http://en.wikipedia.org/wiki/Internet_censorship (accessed 01 July 2013).
15 http://www.calvin.edu/academic/rit/webBook/chapter6/censorship/ (accessed 01 July 2013). In addition it is reported that the government employs thousands of paid commentators who act as ordinary web users to counter criticism of the government. Known as "50 Cent Party" members, these shapers of public opinion are often paid 50 Chinese cents per posting. http://topics.nytimes.com/topics/news/international/countriesandterritories/china/internet_censorship/index.html (accessed 01 July 2013).

An example of technical censorship and probably the best developed system of technical censorship is to be found in China, ironically called also the „Great Firewall of China". The Communist regime blocks Internet content basically by preventing IP addresses from being routed through. The government does not appear to be systematically examining Internet content, though, as this appears to be technically impractical.[16] Still, in 2009, the government pushed - but ultimately backed off from - a rule that would have required the installation of a new software called "Green Dam-Youth Escort" on all new Chinese-made computers. The software would effectively monitor a user's every move.

To sum up, in general, the possible technical methods are reported to be the following:

- IP blocking[17]
- DNS filtering and redirection[18]
- URL filtering[19]
- Packet filtering[20]
- Connection reset.[21]

3 Restriction of the information dissemination on the internet within the EU and Slovakia

Within the EU, it is mainly internal preventive restriction of information dissemination that is taking place, mostly on the level of private individuals and corporations. In respect of external preventive and repressive restrictions it is to be noted that the EU Directive on E-commerce (2000/31/EU) makes also the Internet service providers (private entities, corporations) liable for the content of the websites published on their servers under specific circumstances - as long as the providers are informed of the prohibited content, and despite of that they neglect to remove the harmful content. This can be another source of both internal as well as external restrictions.

One has to discern between various types of Internet service providers (ISPs), though:
ISPs are not only the telecommunication undertakings providing Internet Services. ISPs can be providers of any other Internet services, such as online auction houses (e.g. eBay), but under certain circumstances also a natural person, even a non-entrepreneur, providing any type of Internet (electronic communications) service, such as e.g. admins of chat-forums. Article 2 of the EU Directive on electronic commerce (Directive 2000/31/EU) defines ISPs as any natural or legal person providing an information society service - i.e. electronic communications operators, Internet discussion administrator, and other types of providers of information society services.[22]

The issue of liability of ISPs (leading to internal or external restrictions) arises in relation to:

1. potential breaches of law by the Users to whom the service is being provided,
2. in respect of an activity of the ISP proper.

Sub (1), of importance may be e.g. cases such as issue of ISP liability for copyright or trademark infringement committed by the service Users. This would mean a liability of ISPs for the content of Internet transmissions effectuated by the service Users, i.e. a liability of ISP as someone, who is not the original author of the offending content, but indirectly allows to transport, display or store such content, or otherwise process it. The main reason for the establishment of (co)liability of the ISP for the actions of Users would be that the ISP is usually a single and easily identifiable entity to assert any claims against by the injured parties.

16 http://en.wikipedia.org/wiki/Internet_censorship_in_the_People%27s_Republic_of_China (accessed 01 July 2013).
17 Blocking based on IP (Internet Protocol) address. Every device connected to internet has its unique IP address. This blocking will disable access to all content hosted on this device.
18 DNS will return with non-existing, or false address.
19 Filtering based on scanning destinations URL (Uniform Resource Locator) for banned keywords regardless of request.
20 Communication between computers via network uses small specially formatted units of data called packets. Flow of packets with unencrypted information can be identified and interrupted based on content.
21 Time based blockage follows previously filtered connection.
22 MAISNER, Martin – VANÍČEK, Zdeněk: Odpovědnost za obsah přenosu v elektronických komunikacích. Praha: Wolters Kluwer ČR, 2012, p. 10.

However, soon appeared a counter-argument that the strict liability of ISPs would mean imposing an obligation on ISPs to monitor the content of all the information transmitted. Service providers would have to monitor the content of telephone calls, e-mails contents of users' mailboxes, and the content of all websites, for which they are providing space. The factual impossibility to control such massive amount of information (moreover often anonymously communicated) in information networks, was a strong reason to limit the strict liability of ISPs.[23]

Taking an early example from the USA in this respect, the New York Court dismissed the action in case Cubby Inc. v. CompuServe decided in 1996, stating that CompuServe had neither knowledge nor reason to know of the alleged defamatory statements communicated via its servers.[24] On the other hand, in spite of that, the case Stratton Oakmont, Inc. v. Prodigy Services Co. overruled the precedent and held defendant liable, because it had the technical capability to delete the messages, using a software screening program. It was argued that should the ISPs be exempted from liability, they would have no interest in developing instruments for preventing accidents (e.g. filters). The Stratton case has subsequently been overturned by the Communications Decency Act (CDA) of 1996. Section 230(c) (1) stated that: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider". The wide provision of the Sec. 230 has produced a complete immunity for ISPs. A new US legal regulation in the Digital Millennium Copyright Act on the other hand limited this immunity and stated that ISPs are not liable as long as they act merely as intermediaries (in the sense that they do not cooperate and do not select the contents offered on the web sites).[25]

After evaluating this U.S. development, the EU undertook to regulate the issue in detail in its Directives. A sound compromise was reached between the immunity and liability of the ISPs for the content communicated by the Users - namely, the following types of ISPs and service provider liability were discerned in the EU e-Commerce Directive:

a) Internet access providers' (IAPs) liability. The role of access providers is limited to guaranteeing access to Internet content for their customers, even though in fact they may (and in Slovakia they do) provide also other Internet services. As far as they are not interfering with the data, they are considered immune from the liability under the EU E-Commerce Directive. Hence, they are not effectuating any type of information restrictions. They could become liable only e.g. should they interfere with the transmitted data, breach technical standards or be causing a more than temporal storing of data.[26] An important rule is thereby that the IAP is not obliged to monitor the information nor entitled to seek information that is transmitted or stored. If, however, IAP becomes aware of illegality of such information, provider is required to remove these from the electronic communications network, or at least prevent access to them. The court may also order a provider to remove the information from an electronic communications network, even if the provider did not gain knowledge of their illegality.

b) Host providers' liability (also known as host service providers, being the ISPs proper) is liability of intermediaries, whose role is more complex than that of the access providers. Host providers provide space on the hard disc of their computers (servers) for hosting websites and make them available on the Internet."/> Similarly, they are liable for the User's data transmitted or stored only should they gain the knowledge of illegality of an activity taking place within their hosting range of competence. E.g. a domain registry authority (in Slovakia, this is SK-Nic) could according to some views be held liable for illegal conduct of the applicants registering domains, from the moment onwards that the registry gains knowledge of the illegal conduct. Thus, a national domain name registry can be considered a host provider.[27] Similar approach is being taken by some authors towards the search engines, claiming that these perform (provide) an Internet service, in the position of a host provider (albeit sometimes being also referred to as "referencing service providers").[28]

With respect to liability for illegal content that the ISP gains knowledge of, an important issue is the taking down of data or websites by the ISPs upon information on illegal content. Since generally it is not regulated in the EU E-Commerce Directive nor in the Slovak Act on e-Commerce what should be considered illegal, or whether a court decision or any other authoritative decision is required on the illegality of materials, the ISPs sometimes take down materials based on a simple request by anyone, being preventively cautious about their potential liability. This may then lead to a sort of preventive censorship/restrictions and may give rise to potential claims against the ISPs from those whose material was taken down without any proper reason (e.g. if it is shown subsequently that the material was not illegal).

c) Content providers' liability. The content providers are not intermediaries. In contrast, they select or modify information transmitted or stored on the Internet. In other words, they distribute the information, and making a comparison with the "analogue" world, they can be considered actual publishers.[29] They are fully liable for any breach or illegal conduct in relation to the data stored or transmitted. E.g., should they make copyrighted work available as part of a Web page on the Internet, this could lead to copyright infringement, namely of the author's right of communication of copyrighted work to the public. It is not even decisive whether the content provider knew or not that the work was protected by copyright.[30]

The Slovak Act on electronic commerce in its Sec. 6 regulates the ISP liability together with the IAP liability, as already explained, taking into account the E-Commerce Directive rules, further elaborated in the Court of Justice of the EU (hereinafter "CJ EU") case law. Thus, all the above explanation applies fully to Slovakia: hosting providers are not responsible for information provided or transmitted by recipients of the service and stored on to electronic memory devices used for information retrieval, only where the service provider is not aware of illegal content being stored or communicated. Still, the ISPs are not obliged to monitor the information or entitled to seek information that is transmitted or stored. This may hence serve as an important preventive restricting tool, and – failing that – also an important external repressive restricting tool.

Additional preventive and also repressive non-technical restrictions in Slovakia take the form of legal regulation in the Slovak Criminal Code, which punishes both acts of slander and libel if executed via any public media (i.e. including Internet), and also punishes the website content related to Nazism or Holocaust denial, as well as the so-called Jáchymov denial, which is a denial of communist repressions in Czechoslovakia.

A rare case of external technical restrictions (blocking) is the idea of blocking the websites of foreign companies offering betting and gambling services, in order to prevent the citizens of certain European countries to take part in the online-gambling. The reason hidden behind is the protection of population against gambling and the idea of preventing the countries ´ loss of profits from betting. Since these reasons are dubious, taking into account the state recognition and often even support of betting and gambling within its own territory, and moreover CJ EU not respecting the lost profit as a valid argument, the proposals of laws aimed at preventing the provision of online-gambling services from abroad were abandoned both in the Czech Republic and Slovakia in 2011 upon pressures from the EU Commission.[31]

Besides official governmental restrictions of information dissemination on the Internet, private corporations in the Czech Republic and Slovakia also do technically filter harmful content such as child pornography, extremist websites and other harmful content. Providers performing such restrictions in the territory of Czech Republic and Slovakia are mainly the following ones:

- Telefónica O2 (ČR)
- Vodafone (ČR)
- Praha 5 NET (ČR)
- Orange (SR)
- T-Mobile/T-Com (SR)
- Praha 4 Bezdrátová
- O2 (SR)
- T-Mobile (ČR)
- Praha9net (ČR)
- ePraha8 (ČR)

All the mentioned providers block websites from the list drawn up by the British organization called Internet Watch Foundation (IWF), whereby the list is not publicly accessible.[32]

23 Ibid., p. 17.
24 RICCIO, Giovanni Maria: Internet Service Providers Liability. In: Introduction To ICT Law (Selected Issues). Ed. by Radim Polčák. Brno: Masarykova universita, 2007, p. 58.
25 Ibid., pp. 58-62.
26 POLČÁK, Radim: Internet a proměny práva. Praha: Auditorium, 2012, p. 148.
27 POLČÁK, Radim: Internet a proměny práva, p. 157 (Praha: Auditorium, 2012).
28 Ibid., p. 161.
29 RICCIO, Giovanni Maria: Internet Service Providers Liability, p. 57.
30 MAISNER, Martin – VANÍČEK, Zdeněk: Odpovědnost za obsah přenosu v elektronických komunikacích, pp. 12-13.
31 Cf. ZÁLOM, Luboš: Internetová svoboda a cenzura v ČR. Available at: http://www.mises.cz/clanky/internetova-svoboda-a-cenzura-v-cr-369.aspx (accessed 01 July 2013).; KVASNICA, Ivan: Američanom hrozí cenzúra internetu. Available at: http://www.zive.sk/americanom-hrozi-cenzura-internetu/sc-3-a-297384/default.aspx (accessed 01 July 2013).
32 http://blok.hrach.eu/ (accessed 01 July 2013).

4 Pros and cons of restraining the information dissemination on the internet

Those opposing restraining the information dissemination and censorship on the Internet mostly complain that filters:

- violate an individual's right to free and full access to information
- violate the website's authors ´ freedom of speech
- impose one person's moral standards on another person
- have technical problems:
  - may block pages that are not necessarily objectionable, such as a page about breast cancer that is blocked because of the word breast.
  - may fail to block a page that is objectionable, such as a page that contains pornographic images but does not contain any banned words
  - reduces performance (loading pages takes longer because they must be checked first)
  - prevents complex web interactions, e.g., may cause trouble with connecting to downloadable software modules
  - banner ads with objectionable material cause the entire page to be blocked[33]
  - finally, they realize that every technical mean developed so far was, or will be, circumvented.

As an example, in 2011 US had mistakenly shut down 84,000 websites, wrongfully accused of having links to child pornography. It took approximately 3 days to get the websites back up and running. In 2012, similar situation took place in Denmark - visitors to Facebook and Google together with approximately 8,000 other websites were shocked when they logged in and were confronted with the following message: "The National High Tech Crime Centre of the Danish National Police [NITEC], who assist in investigations into crime on the Internet, has informed Siminn Denmark A/S, that the Internet page which your browser has tried to contact may contain material which could be regarded as child pornography."[34]

On the other hand, advocates of filtering claim that:

- filtering within a corporation prevents employees from wasting company time; within a school, it prevents children from accessing materials that their parents would find objectionable, inappropriate, or harmful
- allowing individuals to access pornographic materials in a public area could be considered sexual harassment to others that can view the screen
- filters block immoral, harmful, and sometimes illegal materials
- the filter is often imposed by the owner of the equipment, who has the right to dictate the terms of use for the equipment
- it is unreasonable to object that filtering involves imposing one's views on another; in any society, one group's view will always be imposed upon others. The ultimate question is whether the view imposed is the correct one.[35]

Surely, both views are correct to a certain extent. The only correct solution lies in the proportionality of restricting the information dissemination (censorship).

Still, generally, the approach of the EU is against the censorship. European Parliament ´s resolution calls for the European Commission to come up with new rules by 2013 to improve the monitoring of E.U. exports of technology that can be used to censor or block websites and monitor mobile communications. It also wants more accountability for companies that wilfully sell to despotic regimes.[36]

33 http://www.calvin.edu/academic/rit/webBook/chapter6/censorship/ (accessed 01 July 2013).
34 http://digitaljournal.com/article/320602 (accessed 01 July 2013).
35 http://www.calvin.edu/academic/rit/webBook/chapter6/censorship/ (accessed 01 July 2013).
36 http://www.pcworld.com/businesscenter/article/254007/eu_parliament_wants_tighter_monitoring_of_internet_censorship.html (accessed 01 July 2013).

5 In search of proportionality

The U.N. Universal Declaration of Human Rights from 1948 in its Article 19 guarantees the freedom of opinion and expression. This right is also guaranteed by the Charter of Fundamental Rights of the EU in Art. 11, as well as in the Constitution of the Slovak Republic in Art. 26 on the freedom of expression.

In December 2003 the World Summit on the Information Society (WSIS) was convened under the auspice of the United Nations, where the WSIS Declaration of Principles was adopted with the following wording: „4. We reaffirm, as an essential foundation of the Information Society, and as outlined in Article 19 of the Universal Declaration of Human Rights, that everyone has the right to freedom of opinion and expression; that this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers. Communication is a fundamental social process, a basic human need and the foundation of all social organization. It is central to the Information Society. Everyone everywhere should have the opportunity to participate and no one should be excluded from the benefits the Information Society offers."[37]

In the European Convention on Human Rights (ECHR), this freedom is protected by Article 10, with the second paragraph identifying cases where this freedom may be restricted - if it were to undermine "national security, territorial integrity or public safety." Restrictions are also allowed "for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary".[38] These rights and interests are hence found in conflict when it comes to restriction of information dissemination on the Internet.

Who is the one to say when is the national security or protection of health and morals to take precedence, though? It should be courts, of course. Coming back to the ISP restrictions and control of the information shared, the European Court of Justice (today's ´ CJ EU) ruled in the decisions SABAM v. Scarlet and SABAM v. Netlog[39] that forcing Internet service providers to monitor and censor their users' communications violates the EU law, and in particular the right to freedom of communication.[40] In further search of balance, the CJ EU in the Netlog case used the balancing test established already in the Scarlet/SABAM (C-70/10), and based its decision on both the E-Commerce Directive (2000/31/EC) and on the Charter of Fundamental Rights of the EU, concluding that the business freedom of hosting providers and the interests of the society as a whole cannot be counterbalanced with the interests of only one part of industry (e.g. the intellectual property rights holders). Hence, it should not be the ISPs to be forced to decide on illegality and proportionality of restrictions in the meaning of a duty to monitor the information dissemination and to censor it.

This is in line with the older case law of the CJ EU in case C-60/00 (Carpenter), where the CJ EU formulated four conditions of admissibility of interference with fundamental rights:

- The legal basis (legality);
- A legitimate interest (legitimacy);
- Measure must be necessary in a democratic society – there must be present a pressing social need;
- Adequacy (proportionality) in relation to the intended objective.[41]

The issue of proportionality was also dealt with in the CJ EU decision in case Fedesa (C-31/88). Based on these decisions, the following aspects should be assessed when considering proportionality:

a. eligibility criteria - whether the measure enables the attainment of the goal;
b. necessity - comparison of restrictive measures with other measures allowing to achieve the same goal, but not limiting the fundamental rights and freedoms; and
c. comparison of the importance of the colliding rights and freedoms – being considered as proportionality in the strict sense.

37 http://en.wikipedia.org/wiki/Right_to_Internet_access (accessed 01 July 2013).
38 Net Filtering Violates the Rule of Law. Available at: http://www.laquadrature.net/en/Net_Filtering (accessed 01 July 2013).
39 Cf. http://edri.org/sabam_netlog_win (accessed 01 July 2013). The wording of the questions was the same in both cases except that the Netlog decision specifically addresses the situation of hosting providers, while the Scarlet case involved Internet access providers.
40 http://www.laquadrature.net/en/Net_Filtering (accessed 01 July 2013).
41 BULLA, Martin: Ochrana súkromia zamestnancov optikou judikatúry Súdneho dvora Európskej únie. In: BARANCOVÁ, Helena et al.: Monitorovanie zamestnancov a právo na súkromný život. Bratislava : Sprint dva, 2010, p. 74.

Proportionate action should therefore be:

- Capable
- Essential
- The least burdensome.[42]

These findings can be applied also to the question of interference with the freedom of speech / expression: proportionality is assessed by necessity, respectively possibility of other options to achieve the same goal, while minimizing interference with the freedoms, and also by the capability to achieve the desired goal. Disproportionality is seen e.g. in a situation when Wikipedia was blocked for almost three days in late 2008 and blacklisted by the Internet Watch Foundation (IWF), as a result of the publication of the original cover art of the album "Virgin Killer" by the rock band Scorpions, released in 1976. Similarly disproportionate would be to require from the ISPs to monitor their Users communication.

In line with the proportionality assessment criteria, an independent think-tank proposes there are at least two other measures which are far more satisfying than the blocking measures required from the ISPs: The first is the removal of content from the hosting servers at judicial request, which should be improved through international judicial cooperation; and the second one is the possibility for users (parents) to install private filtering systems on their computers to block access to specific online content.[43] Hence, private preventive measures should be applied, and - failing that, judicial protection should be guaranteed.

6 Conflict of laws and jurisdiction issues in case of damage caused by information dissemination

In relation to legal transactions and legal acting in the cyberspace, it should be noted that time and space take different forms in the cyberspace, which plays a role also in the judicial cooperation and ISP liability in respect of information restrictions. Let us take the example of time in case of slander and libel in the common law system – does defamation in cyberspace represent a one-time act or is it a long-lasting act? Slander is namely a one-time, spoken defamation, while Libel is an enduring, usually written defamatory statement. The information presented in the cyberspace only once may be preserved there virtually forever, disregarding the changing standards of legality depending from the valid legislation.

Concerning the twisting of space in the cyberspace, due to the non-existence of borders as another specific sign of cyberspace, cross-border relations pose a challenge to the traditional concepts of conflict of laws and to the rules establishing jurisdiction of national courts. In the USA, the milestones in the development of the concept of Internet jurisdiction (combining applicability of law and jurisdiction of courts in one)[44] were the Dow Jones vs. Gutnick case preferring as a decisive factor the place, where the information is downloaded from the Internet, and later a case of Zippo Mfr. Co. vs. Zippo Dot Com case, discerning between active, passive (not establishing the jurisdiction of the court) and interactive websites.[45]

42 MORÁVEK, Jakub: Možnosti monitorování zaměstnanců na pracovišti v právním řádu České republiky. In: Ibid., p. 49.
43 Net Filtering Violates the Rule of Law. Available at: http://www.laquadrature.net/en/Net_Filtering (accessed 01 July 2013).
44 POLČÁK, Radim – ŠKOP, Martin – MACEK, Jakub: Normativní systémy v kyberprostoru (úvod do studia). Brno: Masarykova univerzita, 2005, p. 31. Cf. Statement of Minnesota Attorney General on Internet Jurisdiction, http://cyber.law.harvard.edu/ilaw/Jurisdiction/Minnesota_Full.html (accessed 01 July 2013).
45 POLČÁK, Radim – ŠKOP, Martin – MACEK, Jakub: Normativní systémy v kyberprostoru (úvod do studia). High Court of Australia, Dow Jones and Company Inc v Gutnick [2002], http://www.austlii.edu.au/au/cases/cth/high_ct/2002/56.html (accessed 01 July 2013). Zippo Mfr. Co. v. Zippo Dot Com, Inc., http://cyber.law.harvard.edu/metaschool/fisher/domain/dncases/zippo.htm (accessed 01 July 2013).

In the EU, the Brussels I[46] and II[47] Regulations of the EU set the rules of establishing jurisdiction of courts, and the Rome I[48] and II[49] Regulations regulate the conflict of law rules. As far as the applicable law in private liability cases is concerned (causing harm by information disseminated via Internet), this is regulated by the EC Regulation 864/2007 (the Rome II Regulation) on the law applicable to non-contractual obligations. In case of tort/delict (in Slovakia construed as liability for damage), the applicable law shall generally be (based on the Rome II Regulation) the law of the country in which the damage occurs, irrespective of the country in which the event giving rise to the damage occurred and irrespective of the country or countries in which the indirect consequences of that event occurred, unless the parties agree otherwise. However, if the person who is claimed to be liable and the person sustaining damage both had their habitual residence in the same country at the time when the damage arose, the law of that country is to be applied notwithstanding where the damage arose. Finally, if it is clear from the circumstances of the case that the illegal act is more closely connected to other country (e.g. based on an existing contractual relationship); the law of that other country shall apply. Hence, in respect of liability, the following general scheme as offered by Reimann for Germany (under the Rome II Regulation), can upon certain modification be applied to Slovakia as well in order to determine the applicable law:

1. Choice of law by the parties
2. Significantly strong connection with a specific contractual relationship or a specific country
3. Common place of residence of the parties
4. Choice by the damaged person of the law of the place of injury/damage, or finally,
5. Place of wrongful act.[50]

As far as the jurisdiction (meaning to determine the courts of which country are competent) is concerned, this issue is currently addressed by the Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (Brussels I), establishing the basic principles of EU Member States' jurisdiction (a recast Regulation will be effective as of January 2015). Under Brussels I, in general, it is for the seat of the defendant to establish where to file a civil law action (Art. 2 para. 1). The seat of the company (or a natural person's residence) is thus important rather than the location of a server. However, a problem may arise to identify the perpetrator and the seat (residence) of the perpetrator, especially in case of peer-to-peer networks and in case no international cooperation is in place with the specific country of offender's residence.

In case of harm, the courts of the place where harmful effect occurred may additionally claim competence (Art. 5 para. 3). The "harmful effect" occurs both in the place where e.g. infringing copyrighted work is accessed or distributed, as well as in place where the offender committed the harmful conduct (potentially the country of the seat of publisher / uploader), as stated originally in the CJ EU Shevill case. In joint judgment in E-Date Advertising and Martinez cases (C-509/09 and C-161/10) this was tested under the online-circumstances of the case. The CJ EU concluded[51] that in the event of an alleged infringement by means of content placed online on an Internet website, the person who considers that their rights have been infringed has the option of bringing an action for liability, in respect of all the damage caused, either

1. before the courts of the Member State in which the publisher of that content is established or
2. before the courts of the Member State in which the centre of their interests is based, or
3. before the courts of each Member State in the territory of which content placed online is or has been accessible. Those courts have jurisdiction only in respect of the damage caused in the territory of that Member State, though.[52]

46 Council Regulation (EC) No. 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters.
47 Council Regulation (EC) No. 2201/2003 of 27 November 2003 concerning jurisdiction and the recognition and enforcement of judgments in matrimonial matters and the matters of parental responsibility, repealing Regulation (EC) No. 1347/2000.
48 Regulation (EC) No. 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I).
49 Rome II Regulation (EC) No. 864/2007 on the law applicable to non-contractual obligations.
50 SVANTESSON, Dan Jerker B.: Private International Law and the Internet. Alphen: Wolters Kluwer, 2012, p. 216.
51 CUNIBERTI, Gilles: ECJ Rules in E-Date Advertising and Martinez, http://conflictoflaws.net/2011/ecj-rules-in-e-date-advertising-and-martinez/ (accessed 01 July 2013).
52 SAVIN, Andrej: Jurisdiction in Electronic Contracts and Torts – the Development of the European Court's Case Law, p. 15,

(Note: This would mean that courts of three different countries could be competent, deciding on the whole amount of damages in cases sub 1.) and 2.) or on the proportional part of damages relevant to the specific country in case sub 3.). In combination with the rules on applicable law under Rome II (see supra), these three different courts would probably always apply their national law under pretext that it is the law of the country where the harm occurred, or could resort to the 'effect' method, applying the law of the country most affected by the illegal conduct).

Criminal jurisdiction is somewhat specific – here the jurisdiction and conflict of laws rules blend in one and the determination of applicable law and competent court is governed by various theories – of territoriality, nationality, universality or protection – making sure that the jurisdiction of national courts and applicability of national criminal law is given in most cases should there be any slightest link to the country, its territory, its interests or its citizens. However, not always if an act is punishable under the Slovak Criminal Code (i.e. when the Slovak criminal law is applicable), and jurisdiction of Slovakian courts is given, the Slovak authorities of criminal procedure can successfully start and finish the proceedings. There are certain limits to the actual proceedings – e.g. racist and other hate-related websites that are written in Slovak and are publicly accessible, might be placed on the servers of Internet providers in the U.S., where there is different legal environment, and the promotion and further dissemination of racist or Nazi-related speech is not criminalized there. In the event that this is a website on a U.S. server, the U.S. authorities usually refuse to cooperate in criminal proceedings because the First Amendment of the U.S. Constitution (freedom of expression) does not allow them to punish the creator of this website or to force him to give out any information. This results in a factual impossibility of detection and punishment of the actual perpetrators within the USA.5[53] Rather rare in this respect is the Tore Tvedt case, where a Norwegian was sentenced by a Court in Norway for having stored his webpage with a racist and anti-Semitic content on a U.S. server.[54] In this case, the Norwegian authorities had the citizen present in Norway, and they were able to prove his direct connection with the website.

Finally, even in case of a successful criminal proceeding leading to conviction of a foreigner, still, the recognition of the decision (judgment) in the country of the residence or seat of the convicted may be hampered. An example is the case UEJF et Licra c/a Yahoo! Inc et Yahoo France, where the decision of French authorities was disrespected under the U.S. jurisdiction due to the broader guarantees for freedom of speech in the U.S., protecting also the anti-Semitic and Nazi-related Internet contents.56

These troubles could be spared in case the cooperation would be more intense in the area of cybercriminal procedural law and punishment. That was the idea behind the 2001 Cybercrime Convention's articles on international cooperation and mutual assistance.

Conclusions

Restriction of information dissemination on the Internet has various facets and follows various goals. In general, in democracies, restriction of information dissemination is only allowed upon meeting the standards of balanced rights, freedoms and interests – freedom of expression/speech, the protection of rights and freedoms of other human beings (including intellectual property rights), and the national security and public policy interests. Proportionality has to be always taken into account in order not to disproportionately limit fundamental rights, which comprise at least the freedom of speech/expression, if not also the right to Internet. Besides official external preventive and repressive, technical or non-technical (e.g. legislative) restrictions, however, private restriction of information dissemination is also present - mostly in the form of preventive internal restrictions under the threat of legal action or criminal prosecutions. However, this may sometimes lead to premature decisions of blocking and taking-down websites without proper reasons in order to prevent liability by the Internet service providers under the e-commerce Directive and the Slovak e-commerce Act. More proportionate solutions could be found instead, mostly in the form of strengthening the international police and judicial cooperation as a repressive external tool, while preserving the necessary and reasonable preventive autonomous restriction.

http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1919651 (accessed 01 July 2013).

53 HERCZEG, Jiří: Extremismus a hranice svobody projevu na internetu. In: Český právní řád a ochrana kyberprostoru (vybrané problémy). Praha: Univerzita Karlova v Praze, Nakladatelství Karolinum, 2008, p. 38.

54 COTTIM, Armando A.: Cybercrime, Cyberterrorism and Jurisdiction. An Analysis of Article 22 of the Coe Convention on Cybercrime. In: Law and Technology: Looking into the Future: Selected Essays. Ed. by Meritxell Fernández-Barrera et al. Florence: European Press Academic Publishing, 2009, p. 85.

LITERATURE:

ACLU. ACLU Disappointed in Ruling on Internet Censorship in Libraries, But Sees Limited Impact for Adults. Available on the Internet: American civil liberties union: http://www.aclu.org/technology-and-liberty/aclu-disappointed-ruling-internet-censorship-libraries-sees-limited-impact-ad

ACLU. Internet Censorship. Available on the Internet: American civil liberties union: http://www.aclu.org/free-speech/internet-censorship

ADAMOVÁ, Karolína: Cenzurní zásahy do české kultury v letech 1948-1989. In: Vývoj práva v Československu v letech 1945-1989. In K. MALÝ, L. SOUKUP, Vývoj práva v Československu v letech 1945-1989 (s. 281-306). Praha: Karolinum.

Associated Press in Beijing. Free market thinktank's website shut down in China. Available on the Internet: The Guardian: http://www.guardian.co.uk/world/2012/may/02/free-market-thinktank-website-shut-china

BAKER, Jennifer: EU Parliament Wants Tighter Monitoring of Internet Censorship. Available on the Internet: PCWorld: http://www.pcworld.com/article/254007/eu_parliament_wants_tighter_monitoring_of_internet_censorship.html

BELL, Melissa: The Washington Post. Available on the Internet: What Internet censorship looks like around the world: http://www.washingtonpost.com/blogs/blogpost/post/internet-censorship-what-does-it-look-like-around-the-world/2012/01/18/gIQAdvMq8P_blog.html

BULLA, Martin: Ochrana súkromia zamestnancov optikou judikatúry Súdneho dvora Európskej únie. In Helena BARANCOVÁ, et al., Monitorovanie zamestnancov a právo na súkromný život (s. 74). Bratislava: Sprint dva.

Calvin College. Chapter 6: Social and Ethical Issues: Internet Censorship. Available on the Internet: Calvin College. http://www.calvin.edu/academic/rit/webBook/chapter6/censorship/

CASO, Frank: Censorship. New York: Facts On File.

COTTIM, Armando A.: Cybercrime, Cyberterrorism and Jurisdiction. An Analysis of Article 22 of the Coe Convention on Cybercrime. In: Law and Technology: Looking into the Future: Selected Essays. Ed. by Meritxell Fernández-Barrera et al. Florence: European Press Academic Publishing, 2009.

CUNIBERTI, Gilles: ECJ Rules in E-Date Advertising and Martinez, http://conflictoflaws.net/2011/ecj-rules-in-e-date-advertising-and-martinez/

DRGONEC, Ján: Masmediálne právo na Slovensku v ére digitalizácie elektronických masmédií. In: Communication Today, 2, 2011, 2, pp. 20-33. DSL.sk. T-Mobile začal blokovať nelegálne stránky. Available on the Internet: DSL.sk: http://www.dsl.sk/article.php?article=8340 European Digital Rights. SABAM vs Netlog - another important ruling for fundamental rights . Available on the Internet: European Digital Rights: http://edri.org/sabam_netlog_win

GÁBRIŠ, Tomáš: Definícia veci a výzvy modernej vedy. In: Justičná revue, 60, 2008, pp. 529-40.

HERCZEG, Jiří: Extremismus a hranice svobody projevu na internetu. In: Český právní řád a ochrana kyberprostoru (vybrané problémy). Praha: Univerzita Karlova v Praze, Nakladatelství Karolinum, 2008.

High Court of Australia, Dow Jones and Company Inc v Gutnick [2002], http://www.austlii.edu.au/au/cases/cth/high_ct/2002/56.html

HRACH, Jan: Poskytovatelé, kteří cenzurují Internet. Available on the Internet: blok.hrach.eu: http://blok.hrach.eu/

KVASNICA, Ivan: Američanom hrozí cenzúra internetu. Available on the Internet: živé: http://www.zive.sk/americanom-hrozi-cenzura-internetu/sc-3-a-297384/default.aspx

La Quadrature du Net. CETA, the Zombie ACTA, Must Face the Same Fate. Available on the Internet: La Quadrature du Net: http://www.laquadrature.net/en/ceta-the-zombie-acta-must-face-the-same-fate La Quadrature du Net. Net Filtering. Available on the Internet: La Quadrature du Net: http://www.laquadrature.net/en/Net_Filtering

MAISNER, Martin – VANÍČEK, Zdeněk: Odpovědnost za obsah přenosu v elektronických komunikacích. Praha: Wolters Kluwer ČR, 2012.

MORÁVEK, J. Možnosti monitorování zaměstnanců na pracovišti v právním řádu České republiky. In H. BARANCOVÁ, et al., Monitorovanie zamestnancov a právo na súkromný život (s. 49). Bratislava: Sprint dva.

NUNEZ, Michael: Internet Censorship: Is the Internet a Human Right? Available on the Internet: International Business Times: http://www.ibtimes.com/internet-censorship-internet-human-right-212821
NY Times. Internet Censorship in China. Available on the Internet: The New York Times: http://topics.nytimes.com/topics/news/international/countriesandterritories/china/internet_censorship/index.html
POLČÁK, Radim: Internet a proměny práva. Praha: Auditorium, 2012.
POLČÁK, Radim – ŠKOP, Martin – MACEK, Jakub: Normativní systémy v kyberprostoru (úvod do studia). Brno: Masarykova univerzita, 2005.
RICCIO, Giovanni Maria: Internet Service Providers Liability. In: Introduction To ICT Law (Selected Issues). Ed. by Radim Polčák. Brno: Masarykova universita, 2007.
RININSLAND, Ændrew: Internet censorship listed: how does each country compare? Available on the Internet: The Guardian: http://www.guardian.co.uk/technology/datablog/2012/apr/16/internet-censorship-country-list
ROBINSON, B. Internet censorship software programs. Available on the Internet: Religious Tolerance: http://www.religioustolerance.org/cyberpat1.htm
SAVIN, Andrej: Jurisdiction in Electronic Contracts and Torts – the Development of the European Court's Case Law, p. 15, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1919651
SEWELL, Anne: Op-Ed: Internet censorship and how it can affect innocent websites. Available on the Internet: Digital Journal: http://digitaljournal.com/article/320602 Statement of Minnesota Attorney General on Internet Jurisdiction, http://cyber.law.harvard.edu/ilaw/Jurisdiction/Minnesota_Full.html
SVANTESSON, Dan Jerker B.: Private International Law and the Internet. Alphen: Wolters Kluwer, 2012.
Wikipedia. Internet censorship. Available on the Internet: Wikipedia: http://en.wikipedia.org/wiki/Internet_censorship
Wikipedia. Internet censorship in the People's Republic of China. Available on the Internet: Wikipedia: http://en.wikipedia.org/wiki/Internet_censorship_in_the_People%27s_Republic_of_China
Wikipedia. Zensur im Internet. Available on the Internet: Wikipedia: http://de.wikipedia.org/wiki/Zensur_im_Internet
ZÁLOM, Luboš: Internetová svoboda a cenzura v ČR. Available on the Internet: Ludwig von Mises Institut: http://www.mises.cz/clanky/internetova-svoboda-a-cenzura-v-cr-369.aspx
Zippo Mfr. Co. v. Zippo Dot Com, Inc., http://cyber.law.harvard.edu/metaschool/fisher/domain/dncases/zippo.htm