МЕЃУНАРОДНА НАУЧНА КОНФЕРЕНЦИЈА

БАЛКАНОТ МЕЃУ МИНАТОТО И ИДНИНАТА: БЕЗБЕДНОСТ, РЕШАВАЊЕ НА КОНФЛИКТИ И ЕВРОАТЛАНТСКА ИНТЕГРАЦИ

INTERNATIONAL SCIENTIFIC CONFERENCE

THE BALKANS BETWEEN PAST AND FUTURE: SECURITY, CONFLICT RESOLUTION AND EURO-ATLANTIC INTEGRATION

МЕЃУНАРОДНА НАУЧНА КОНФЕРЕНЦИЈА

БАЛКАНОТ МЕЃУ МИНАТОТО И ИДНИНАТА: БЕЗБЕДНОСТ, РЕШАВАЊЕ НА КОНФЛИКТИ И ЕВРОАТЛАНТСКА ИНТЕГРАЦИЈА

05-08 Јуни 2013, Охрид

Том I

СКОПЈЕ, 2013

INTERNATIONAL SCIENTIFIC CONFERENCE

THE BALKANS BETWEEN PAST AND FUTURE: SECURITY, CONFLICT RESOLUTION AND EURO-ATLANTIC INTEGRATION

05-08 June 2013, Ohrid

Volume I

SKOPJE, 2013

Издавачи:
Универзитет „Св. Климент Охридски“ Битола
Факултет за безбедност – Скопје

За издавачите:

проф. д-р Златко Жоглев, ректор на Универзитетот „Св. Климент Охридски“ – Скопје
проф. д-р Оливер Бачановиќ
Декан на Факултетот за безбедност – Скопје

Уредник на изданието:
Проф. д-р Цане Мојаноски

Преведувачи:
Анче Белада
Александра Тодору
Марија Рашковска Георгиевска

Компјутерска обработка:
Проф. д-р Цане Мојаноски
Оливера Трајанова
Корица: Кире Лазаревски

Печати:
АД „Ван Гог“ - Скопје

Адреса на издавачите:
Факултет за безбедност
1000 Скопје
П. Фах 103
тел: 022546211

Универзитет „Св. Климент Охридски“
1ви Мај б.б.
7000 Битола,
тел: 047223788

Publishers:
University “St. Kliment Ohridski”- Bitola
Faculty of Security- Skopje

For the Publishers:

Dr. sc. Zlatko Žoglev, Rector of the University “St. Kliment Ohridski”- Bitola
Dr. sc. Oliver Bacanovic, dean of the Faculty of Security- Skopje

Editor in Chief:
Dr. sc. Cane Mojanoski

Proofreading:
Anche Belada
Aleksandra Todoru
Marija Raškovska Georgievska

Layout design:
Dr. sc. Cane Mojanoski
Olivera Trajanova
Kire Lazarevski

Print:
“Van Gog” - LTD Skopje

Address of the Publishers:
Faculty of Security
1000 Skopje
P.O. Box 103
tel: ++389(0)22546211

University “St. Kliment Ohridski”
1 Maj b.b.
7000 Bitola
tel: +++389(0) 47223788

PROGRAMME COMMITTEE

Dr. Sc. Snezana Nikodinovska Stefanovska, Faculty of Security
Prof. Dr. Sc. Jean-Michel Waele, Dean of the Faculty of Social and Political Sciences at Université Libre from Brussels, Belgium
Dr. Sc. Dzemal Sokolovic, Retaired professor from University of Bergen, Norway Director of Institut for Strengthening Democracy in Bosnia, BiH
Dr. Sc. Goran Milošević, Dean of the Academy of Criminalistics and Police Studies, Serbia
Helene Martini, President of the Association of European Police Colleges
Dr. Sc. Tatyana Malyarenko, Donetsk University of Management, Ukraine
Dr. Sc. Oliver Bačanović, Faculty of Security
Dr. Sc. Gorazd Meško, Dean of the Faculty of Criminal Justice and Security, Slovenia
Dr. Sc. Wieslav Chizovicz, University of Economics in Warsaw
Dr. Sc. Cane Mojanoski, Faculty of Security
Dr. Sc. Yordan Penev, Rector of the Academy of the Ministry of Interior, Bulgaria
Dr. Sc. Radomir Milašinović, Dean of the Faculty of Security Studies, University of Belgrade, Serbia
Dr. Sc. Vladimir Ortakovski, Faculty of Security
Dr. Sc. Remzi Findikli, Director of the Turkish National Police Academy, Turkey
Dr. Sc. Mile Šikman, Head of the Administration for Police Education of Republika Srpska, Bosnia and Herzegovina
Živko Šipčić, Director of the Police Academy, Montenegro
Dr. Sc. Geogre Popa, Rector of the Police Academy "Alexandru Ioan Cuza", Romania
Dr. Sc. Nedžad Korajlić, Dean of the Faculty of Criminalistics, Criminology and Security Studies, University of Sarajevo, Bosnia and Herzegovina
Dr. Sc. Ferenc Banfi, Director of CEPOL (European Police College)
Dr. Sc. Zvonimir Dujmović, Dean of the Higher Police School, Croatia

ПРОГРАМСКИ ОДБОР

Проф д-р. Снежана Никодиновска Стефановска, Факултет за безбедност
Проф. д-р. Jean-Michel Waele, Декан на Факултетот за социјални и политички науки на Универзитетот Libre од Брисел, Белгија
Проф. д-р Dzemal Sokolovic, Retaired professor from University of Bergen, Norway Director of Institut for Strengthening Democracy in Bosnia, BiH
д-р Горан Милошевиќ, декан, Криминалистичко-полициска академија, (КПА), Србија
Helene Martini, President of the Association of European Police Colleges
Проф. д-р Tatyana Malyarenko, Donetsk University of Management, Ukraine
Проф. д-р. Оливер Бачановиќ, Факултет за безбедност
д-р Горзд Мешко, декан, Факултет за безбедносни студии, Словенија
Проф. д-р Wieslav Chizovicz, Универзитет за економија, Варшава
Проф. д-р. Цане Мојаноски, Факултет за безбедност
д-р Јордан Пенев, Ректор на Академијата на МВР, Бугарија
Проф. д-р Radomir Milašinović, Декан на Факултетот за безбедносни науки, Универзитет Белград, Србија
Проф. д-р Владимир Ортаковски, Факултет за безбедност
Проф. д-р Remzi Findikli, Директор на турската национална полициска академија, Турција
д-р Миле Шикман, началник, Директорат за полициска едукација, МВР, Република Српска, БиХ
Živko Šipčić, Директор на Полициска академија, Црна Гора
Проф. д-р Geogre Popa, Ректор на Полициска Академија "Alexandru Ioan Cuza", Романиа
Проф. д-р Nedžad Korajlić, Декан на Факултетот за Криминалистика, Криминологија и Безбедносни науки, Универзитет Сараево, Босна и
Проф. д-р Ferenc Banfi, Директор на CEPOL (European Police College)
д-р Звонимир Дујмовиќ, Висока полициска школа на МВР, Хрватска

СЕКРЕТАР

Доц. д-р Никола Дујовски,
Факултет за безбедност –Скопје,
Република Македонија

ОРГАНИЗАЦИОНЕН ОДБОР

проф. д-р Цане Мојаноски,
претседател
проф. д-р Борис Мургоски
проф. д-р Миодраг Лабовиќ
доц. д-р Снежана Мојсоска
доц. д-р Драгана Батиќ
доц. д-р Марија Миленковска
асс. м-р Раде Рајковчевски

СЕКРЕТАР
асс. м-р Марјан Ѓуровски

SECRETARY

Dr. sc. Nikola Dujovski, Faculty of Security-Skopje, Republic of Macedonia

ORGANIZING COMMITTEE

Prof. Cane Mojanoski, PhD, President
Prof. Boris Murgoski, PhD
Prof. Miodrag Labovich, PhD
Prof. Snezana Mojsoska, PhD
Prof. Dragana Batich, PhD
Prof. Marija Milenkovska, PhD
Ass. Rade Rajkovcevski, MA

SECRETARY
Ass. Marjan Gjurovski, MA

Contents

SECURITY DILEMMAS AND GEOPOLITICAL TRENDS IN INTERNATIONAL RELATIONS WITH PARTICULAR REFERENCE TO MIDDLE EAST, EASTERN EUROPE AND WESTERN ASIA

SECURITY IN THE ERA OF SMART TECHNOLOGY

CONCEPT AND PRACTICE OF 'CYBER HATE SPEECH' IN INTERNATIONAL AND DOMESTIC LAW

Dr.sc. Zaneta Poposka,
Dr.sc. Jovan Ananiev,

Faculty of Law, University "Goce Delcev" - Stip

Abstract

An issue which is gaining increasing attention is the diffusion of hate on the Internet. The importance of the Internet as a tool for communication, networking and social interaction has dramatically increased over the recent years. At the same time, the Internet has become a tool for dissemination of messages of hatred as well as a platform for bloggers and organized groups to recruit, control their members, organize attacks, and intimidate and harass their opponents. Although it is often difficult to prove the connection between manifestations of hate on the Internet and hate crimes in the real world, there is evidence that the psychological influence of material available on the Internet is quite high, especially on youth.

The aim of this paper is to clarify the concept of cyber hate speech and how this concept is dealt with under the international law and domestic legislation. This paper is also intended to present the contemporary challenges and dilemmas surrounding cyber hate speech, and aims to provide an overview of the criteria followed by the European Court of Human Rights in its case law relating to the right to freedom of expression and its restrictions. Furthermore, the practice involving hate speech on the Internet that have occurred in the country in the past years will be analyzed.

Key words: Hate speech, Internet, legislation

Introduction

With the advancement of new technologies and the Internet, governments are increasingly confronted with the challenge of seeking an appropriate balance between the universal right to freedom of expression and the prohibition of hateful online content. The Internet content regulation remains a major problem as the different approaches of national authorities constitute an obstacle to harmonization efforts at the international level. As a consequence, there are no clear guidelines as to what is acceptable and what is not in terms of the Internet contents. International 'soft law' instruments dealing with cyber hate speech have been adopted. Such instruments sometimes call on States to criminalize hate speech, including hate expressed

speech and aids in increasing the social acceptability of hate in mainstream discourse.

With the widespread availability of the Internet and the increasing number of users, online content regulation has become an important focus of governments and supranational bodies across the globe (OSCE Representative on Freedom of the Media Report, 2010, p. 4). The specific character of the Internet poses however serious challenges to any attempts to regulate its contents. Due to the lack of consensus on the concept of hate speech on the Internet there are no laws on the international level applicable to hate on the Internet, which results in the absence of clear guidelines as to what is acceptable and what is not in terms of contents.

The Internet Service Providers (ISPs) can use and promote Industry codes of conduct, ethical guidelines and principles as a tool for addressing cyber hateful content. Based on such internal standards, ISPs can look at content without making value judgments about a particular type of speech. A good example is offered by Facebook[1]. However, it should not be left to the Internet industry alone and at the sole discretion to decide what is acceptable and what is not in terms of Internet content. The Industry needs clear guidelines based on national and international law (ODIHR Report, 2010, p. 3).

Due to differing approaches to hate-inciting content on the Internet and the diverse criteria among the States for defining the threshold between freedom of expression and criminal behaviour, the impact of criminal legislation and its implementation is limited. Content is often hosted or distributed from outside the jurisdiction in which it is considered illegal, while the extraterritorial enforcement of laws related to Internet content is very difficult and often ineffective. Laws are not necessarily harmonized at the European level, let alone on a wider scale. Furthermore, unlike traditional media, it is often very difficult to establish the identity of authors of the content available online. Material which originates in one country is copied, edited, and shared across national borders, and can be hosted in different countries, subject to different legislation.

International Legal Standards

Various international legal instruments punish hate speech. However, the specific nature of the Internet calls for the adoption of specific

[1] According to part 3 (Safety) point 7 from the Terms of service the user "will not post content that: is hate speech, threatening incites violence..." Furthermore, according to part 5 (Protecting Other People's Rights) point 1 the user "will not post content or take any action on Facebook that infringes or violates someone else's rights or otherwise violates the law".

instruments to combat hate speech promoting racism and violence, which is widely and swiftly disseminated on the web. Although the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), in particular Article 10 that deals with the freedom of expression, remains the main source of reference regarding hate speech, other legal instruments have been adopted by the United Nations, Council of Europe, and European Union in relation to online hate speech.

United Nations

At universal level, Article 19, paragraph 3 of the UN International Covenant on Civil and Political Rights states that the freedom of expression is not absolute rights and it may therefore be subject to certain permissible restrictions, but these shall only be such as are provided by law and are (ICCPR, 1976). As it specifically concerns online hate speech, the Human Rights Committee's General Comment No.34 on Article 19, paragraph 3 refers to the protection of all forms of expression and the means of their dissemination, including audio-visual as well as electronic and Internet-based modes of expression (Paragraph 12). According to the Comment, "any restrictions on the operation of websites, blogs or any other internet-based, electronic or other such information dissemination system, including systems to support such communication, such as internet service providers or search engines, are only permissible to the extent that they are compatible with paragraph 3. Permissible restrictions generally should be content-specific; generic bans on the operation of certain sites and systems are not compatible with paragraph 3. It is also inconsistent with paragraph 3 to prohibit a site or an information dissemination system from publishing material solely on the basis that it may be critical of the government or the political social system espoused by the government." (Paragraph 43)

On 1st June 2011, the UN signed together with the OSCE, the Organization of American States and the African Commission on Human and Peoples' Rights the Declaration on Freedom of Expression and the Internet (the "Declaration"). In its General Principles, the Declaration states as follows: a). Freedom of expression is applied to the Internet, as it does to all means of communication. Restrictions on freedom of expression on the Internet are only acceptable if they comply with established international standards, including that they are provided for by law, and that they are necessary to protect an interest which is recognized under international law (the 'three-part' test); b). When assessing the proportionality of a restriction on freedom of expression on the Internet, the impact of that restriction on the ability of the Internet to deliver positive freedom of expression outcomes must be weighed against its benefits in terms of protecting other interests; ...

d). Greater attention should be given to developing alternative, tailored approaches, which are adapted to the unique characteristics of the Internet, for responding to illegal content, while recognizing that no special content restrictions should be established for material disseminated over the Internet."

Council of Europe

The Additional Protocol to the Cyber-Crime Convention (2001) concerning the Criminalization of Acts of a Racist and Xenophobic Nature Committed through Computer Systems, adopted on 28th January 2003 and entered into force on 1st March 2006, is of particular relevance to the dissemination of messages of hatred through the Internet. According to Article 2, Paragraph 1 of the Protocol, it is defined that "racist and xenophobic material" and stresses that in order to address this phenomenon, the States parties are required to adopt such legislative and other measures as may be necessary to establish as criminal offences under their domestic law, when committed intentionally and without right, a specified set of acts committed through a computer system.

The Council of Europe's Recommendation (2008) 6 on Measures to Promote Respect for Freedom of Expression and Information with Regard to Internet Filters acknowledges the ways in which Internet filters can impact on freedom of expression and information. The recommendation calls on member states to take measures with regard to the Internet filters, in line with a set of guidelines promoting user notification, awareness and control of Internet filters and accountability of the private and public parties involved.

The General Policy Recommendation No. 6 of the European Commission against Racism and Intolerance (ECRI) recommends that the member states "ensure that relevant national legislation applies also to racist, xenophobic and anti-Semitic offences committed via the Internet and prosecute those responsible for this kind of offences". Furthermore, the recommendation stresses the need to: (i) train the law enforcement authorities in relation to the dissemination of racist, xenophobic and anti-Semitic material via the Internet; (ii) support existing anti-racist initiatives on the Internet; (iii) support the self-regulatory measures taken by the Internet industry to combat racism, xenophobia and anti-Semitism on the Internet; and (iv) increase public awareness of the problem of the dissemination of racist, xenophobic and anti-Semitic material via the Internet while paying special attention to awareness-raising among young Internet-users.

European Union

EU Directive on Electronic Commerce (2000) places specific obligations on Internet service providers in regards to the content access. The Directive requires member states to guarantee "safe havens", or limitations of criminal or civil liability, for ISPs, hosting services and other service providers, provided (a) that they do not have "actual knowledge of illegal activity or information" and (b) once notified of such illegalities, they act "expeditiously" to remove or to disable access to the information, known as the "notice and takedown" procedure. The Directive does not regulate the procedural aspects of notice and takedown, which is left to the discretion of member states.

Measures Aimed at Combating Cyber Hate Speech

While the intention of the states to combat illegal activity over the Internet and to protect their citizens from harmful content is legitimate, there are also significant legal and policy developments which sometimes have an unintended negative impact on freedom of expression and the free flow of information. Recent laws and certain legal measures currently under development have provoked much controversy over the past few years. These include access-blocking, filtering and content removal. Before analyzing in detail each of these measures, as explained above, any speech and content related restriction must meet strict criteria under the international law, i.e. 'the three-part test'. The first and most important requirement is that any interference by a public authority with the exercise of the freedom of expression should be lawful. If the interference is "prescribed by law", the aim of the restriction should be legitimate and concern limitations in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health of morals or for the protection of the rights and freedoms of others. Furthermore, any restrictions need to be necessary in a democratic society and the state interference should correspond to a "pressing social need". The state response and the limitations provided by law should be "proportionate to the legitimate aim pursued". Therefore, the necessity of the content-based restrictions must be convincingly established by the state.

Access-blocking measures. Due to the limited effectiveness of criminal laws and lack of harmonization at the international level, a number of states have started to block access to websites and social media platforms allegedly containing illegal content which are located outside their jurisdiction. Blocking access to content seems to be faster, easier and a more convenient solution. Practice shows that access-blocking measures are not

always provided by law nor are always subject to due process principles. Furthermore, blocking decisions are not necessarily taken by the courts and often administrative bodies or the Internet hotlines run by the private sector single-handedly decide which content, website or platform should be blocked. Blocking policies often lack transparency and administrative bodies lack accountability. Appeal procedures are either not in place or they are often not efficient. Therefore, increasingly, the compatibility of blocking with the fundamental right of freedom of expression must be questioned.

The Committee of Ministers of the Council of Europe has urged that "prior control of communications on the Internet, regardless of frontiers, should remain an exception" and that member states "should not, through general blocking or filtering measures, deny access by the public to information and other communication on the Internet, regardless of frontiers" (Committee of Ministers Declaration, 2003, Principle 3). Removal or blocking of access to "clearly identifiable" Internet content is permissible only if "the competent national authorities" have taken "a provisional or final decision on its illegality", provided that all the safeguards of Article 10, paragraph 2 of the ECHR are respected.

It has been argued that under European law and practice, injunctions and orders blocking access to websites should be treated as a method of "prior restraint", and as such should be subject to "the most careful scrutiny." (Open Society Justice Initiative, 2011, p. 3). To be consistent with Article 10, prior restraint regimes must be subject to a particularly strict legal framework, ensuring both tight control over the scope of the bans and effective judicial review to prevent abuse.

Internet blocking orders must be strictly necessary and capable of protecting a compelling social interest. The need for such measures must be convincingly established, and they should be adopted only as measures of last resort. Domestic laws should provide robust and prompt remedies against blocking orders in order to safeguard against unnecessary and disproportionate interferences. European laws generally require pre-blocking notification of ISPs and content providers. It is technically possible to block solely the offending website. Blocking orders that indiscriminately prevent access to an entire group of websites amount to "collateral censorship" should be avoided as unnecessary and disproportionate. The lack of any instances of collateral blocking of large proportions such as of entire web platforms, in the judicial practice testifies to their truly exceptional nature.

Many of the issues described above have been raised in front of the ECtHR in the case Yildirim v. Turkey[2] and Akdeniz v. Turkey. The decision

[2] Namely, a court in Turkey issued an injunction blocking access for all Turkish-based users to the entire Google Sites domain, supposedly to make unavailable a single

of the court will certainly help clarify a number of issues in the area of Internet and freedom of expression, including that of blocking access to websites, and will thus have serious implications for the state parties to the Convention.

Filtering measures. There are various forms of Internet filtering and these may be employed in different contexts. For instance, Internet filtering can take place through URL-based filtering, IP address-based filtering, protocol-based filtering, key-word blocking, filtering on the basis of labeling or rating by the content author or a third party. Internet filters can be applied in the workplace, in public libraries, and schools or at the ISP level. The users' awareness, understanding of, and ability to effectively use Internet filters are key factors which enable them to fully exercise and enjoy their human rights and fundamental freedoms, in particular the right to freedom of expression and information, and to participate actively in democratic processes.

Content-removal measures. In some countries total suspension of communications services, including the Internet access related services is possible in times of war, states of emergency, as well as imminent threats to national security. Legal provisions may allow the authorities to switch off completely all forms of communications, including the Internet communications, under certain circumstances. Research shows that in several States the legal remedy provided for allegedly illegal content is removal or deletion.

Liability of Internet Service Providers (ISPs)

Persons cannot be held criminally liable for any of the offences in the Additional Protocol to the Cyber-Crime Convention 2001, if they do not possess the required intent (Akdeniz, 2008, p. 27 - 29). It is not sufficient, for example, for a service provider to be held criminally liable if such a provider served as a conduit for, or hosted a website or newsroom containing such material, without the required intent under domestic law in the particular case. Moreover, a service provider is not required to monitor conduct to avoid criminal liability.

---

website which included content deemed offensive to the memory of Mustafa Kemal Ataturk, the founder of the Turkish Republic. There is no indication of any attempt by the Turkish authorities to contact or serve notice on Google Inc., the US based owner and operator of Google Sites, prior to issuing the blocking order. A challenge was brought to the ECtHR by the owner of an unrelated academic website that was also blocked by the order, arguing that such an interference with the free flow of information online amounts to "collateral censorship."

The Council of Europe Declaration on the Freedom of Communication on the Internet adopted by the Committee of Ministers on 28th May 2003 provides that member states should not impose on service providers an obligation to monitor content on the Internet to which they give access, that they transmit or store, nor the obligation of actively seeking facts or circumstances indicating illegal activity. Service providers should not be held liable for content on the Internet when their function is limited to transmitting information or providing access to the Internet. However, in cases where the functions of service providers are wider and they store content emanating from other parties, member states may hold them co-responsible if they do not act expeditiously to remove or disable access to information or services as soon as they become aware of their illegal nature. What is important to highlight is that when defining under national law the obligations of service providers, due care must be taken to respect the freedom of expression of those who made the information available, as well as the corresponding right of users to the information.

Although EU member states are prevented from imposing a monitoring obligation on service providers with respect to obligations of a general nature under the EU Directive on Electronic Commerce, this "does not concern monitoring obligations in a specific case and, in particular, does not affect orders by national authorities in accordance with national legislation." (Paragraphs 47 and 48 of the Preamble and Article 15). In most instances liability will only be imposed upon ISPs if there is "knowledge and control" over the information which is transmitted or stored by a service provider. For example, the EU Directive on Electronic Commerce suggests that "it is in the interest of all parties involved in the provision of information society services to adopt and implement procedures" to remove and disable access to illegal information. Therefore, the service providers based in the European Union are not immune from prosecution and liability, and they are required to act expeditiously "upon obtaining actual knowledge" of illegal activity or content, and "remove or disable access to the information concerned" (Paragraph 46).

Although the knowledge and control theory ensures that the information which is transmitted or stored by a service provider is not subject to prior restraint (through monitoring obligations), nonetheless the system is not immune from criticism as studies have shown that, in order not to incur liabilities, ISPs based in Europe tend to remove and take-down content without challenging the notices they receive, which can be problematic and can amount to ex-post censorship (Nas, 2004; Ahlert, Marsden, and Yung, 2003). This concern is also relevant to the Republic of Macedonia where Facebook administrator always acts upon request of the Directorate for Personal Data Protection.

Domestic Legislation

In addition to the general provisions related to hate speech such as Article 417, Paragraph 3[3] and Article 319[4], the Criminal Code of the host country contains provisions addressing hate speech made through a computer system. For example, Article 394-d of the Criminal Code states: "(1) Whosoever via an information system spreads in the public racist and xenophobic written material, photos or other representation of an idea or theory helping, promoting or stimulating hatred, discrimination or violence, regardless against which person or group, based on race, skin color, national or ethnic background, as well as religious belief, shall be sentenced to imprisonment of one to five years." Another provision incriminating online hate speech is Article 173, Paragraph 2: "Whosoever exposes another to a public mockery, by means of an information system, because of his belonging to a group different in its race, skin color, national or ethnic background, or exposes the group of persons characterized with one of these features to mockery, shall be fined or sentenced to imprisonment of up to one year."[5]

According to the Law on Personal Data Protection (Articles 37 and 41), the Directorate for Personal Data Protection has competences to act both as an inspection and a misdemeanour body, and may act on the basis of complaints or on its own motion (ex officio). As an inspection body the Directorate has responsibility over the misuse of personal data.[6] Once the internal procedure is carried out, the Directorate submits a request to the

---

[3] "Whosoever spreads ideas about the superiority of one race over another, or who advocates racial hate, or instigates racial discrimination, shall be sentenced to imprisonment of six months to three years."

[4] "(1) Whosoever by use of force, maltreatment, endangering the security, mocking of the national, ethnic or religious symbols, by damaging other people's objects, by desecration of monuments, graves, or in some other manner causes or excites national, racial or religious hate, discord or intolerance, shall be sentenced to imprisonment of one to five years. (2) Whosoever commits the crime referred to in paragraph 1 by abusing his position or authorization, or if because of these crimes, riots and violence were caused against the people, or property damage to a great extent was caused, shall be sentenced to imprisonment of one to ten years."

[5] Please note that the exposure to mockery through a computer system, as an action of committing the more serious type of insult, consists of crude slight, mockery or inciting contempt for a group or one of its members, precisely because of his or her capacity, by using verbal (oral, written) or real actions (gestures, showing insulting symbols, pictures etc.).

[6] In the course of 2011, the Directorate received 363 complaints (127 of which related to abuse of personal data on the social networks, among which 87 concern fake profiles) related to cases where an account has been compromised. Some of the cases were transferred from the Ministry of Internal Affairs.

administrator of the social network (which in the case of Facebook Europe is located in Dublin) to remove the misused account from the social network. In practice, Facebook administrator always acts upon the Directorate's request. This can lead to arbitrary practice from the national institutions as Facebook administrator is not making value judgments about a particular type of content as being or not "hateful". They are accepting the opinion of the national institutions and are proceeding with deleting a certain user.

While the mandate of the Directorate to act upon individual complaints is straightforward, its authority to act ex officio in case of abuse of social networks to express hate speech is unclear. The modalities through which the Directorate implements this competence are not specified. Although it has been observed that the Directorate co-operates with the Cyber Crime Unit of the Ministry of Internal Affairs in regards to the closure of social networks profiles inciting ethnic and racial hatred, there are no Standard Operating Procedures regulating the form and modalities of such cooperation. This raises serious concern as to whether the practice of access-blocking measures in the host country is in accordance with the law and subject to the principle of due process.

Conclusion

In the past three years, the number of incidents of ethnic and religious intolerance involving hate speech on the Internet has increased in the host country. Although the usage of Facebook and other social networks as a means to express hate speech is to be stigmatised, closure, removal or blocking of social networks accounts, websites, blogs, search engines or any other internet-based, electronic or similar form of communication represents a serious restriction of the right to freedom of expression. Such restrictions on freedom of expression on the Internet are only acceptable if they comply with international standards.

The assessment of the national legislations shows no clear division in the competences between the relevant authorities such as the Ministry of Internal Affairs and the Directorate for personal data protection, as regards removal of Facebook groups or blocking access to websites, blogs and social networks. Further improvement in this area should be a priority.

REFERENCES

Ahlert C., Marsden C., and Yung C. (2003). How 'Liberty' Disappeared from Cyberspace: The Mystery Shopper Tests Internet Content Self-Regulation. Retrieved from http://pcmlp.socleg.ox.ac.uk/text/liberty.pdf.

Akdeniz Y. (2008). The Council of Europe's Cyber-Crime Convention 2001 and the additional protocol on the criminalisation of acts of a racist or xenophobic nature committed through computer systems. Retrieved from http://www.cyber-rights.org/cybercrime/coe_handbook_crcl.pdf.

Anti-Defamation League. (2010). Responding to Cyber hate, toolkit for action. Retrieved from http://www.adl.org/assets/pdf/combating-hate/ADL-Responding-to-Cyberhate-Toolkit.pdf.

Criminal Code, Official Gazette of the Republic of Macedonia, No. 37/1996, 80/1999, 4/2002, 43/2003, 19/2004, 60/2006, 73/2006, 139/2008, 114/2009, 51/2011, 135/2011, 185/2011, 142/2012 and 166/2012, Retrieved from http://www.slvesnik.com.mk.

Committee of Ministers. (2003). Declaration on Freedom of Communication on the Internet.

Council of Europe. (2003). Additional Protocol to the Cyber-Crime Convention concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems. Retrieved from http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm.

Council of Europe (Committee of Ministers) Recommendation (2008)6 on Measures to Promote Respect for Freedom of Expression and Information With Regard to Internet Filters. (2008). Retrieved from http://www.coe.int/t/dghl/standardsetting/media/doc/cm_EN.asp.

Court of Justice of the European Union. (2010). Google France and Google Inc. et al. v Louis Vuitton Malletier et al., Judgment (23 March, 2010) in Joined Cases C-236/08 to C-238/08, OJ C 134. Retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62008J0236:EN:NOT.

Directorate for Personal Data Protection. (2012). Annual Report of the Directorate for Personal Data Protection for 2011. Retrieved from http://www.dzlp.mk/sites/default/files/Dokumenti/Godisen_izvestaj/Godisen_izvestaj_2011.pdf.

European Commission against Racism and Intolerance. (2000). General Policy Recommendation No. 6 on Combating the dissemination of racist, xenophobic and antisemitic materiel via the Internet. Retrieved from http://www.coe.int/t/dghl/monitoring/ecri/activities/gpr/en/recommendation_n6/Rec%206%20en.pdf.

European Court of Human Rights.Yildirim v. Turkey, App no. 3111/10.

European Court of Human Rights. Akdeniz v. Turkey, App no. 20877/10.

European Union. (2000). 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, OJ L 178. Retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:178:0001:0001:EN:PDF.

Facebook's Terms of Service. Retrieved from www.facebook.com/home.php#/terms.php?ref=pf.

Freedom of Expression on the Internet, A study of legal provisions and practices related to freedom of expression, the free flow of information and media pluralism on the Internet in OSCE participating States, commissioned by the Office of the OSCE Representative on Freedom of the Media. (2010). Retrieved from http://www.osce.org/fom/80723.

Human Rights Committee, General Comment No. 34 on Article 19 from the International Covenant on Civil and Political Rights. (2011). CCPR/C/GC/34.

International Covenant on Civil and Political Rights. (1966). Retrieved from http://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-4&chapter=4&lang =en.

Law on Personal Data Protection, Official Gazette no. 7/05, 103/08, 124/10 and 135/11. Retrieved from http://www.slvesnik.com.mk.

Nas S. (2004). Bits of Freedom. Retrieved from www.bof.nl/docs/researchpaperSANE.pdf.

ODIHR. (2010). Report of OSCE-ODIHR activities on hate on the internet, ODIHR.GAL/77/10. Retrieved from http://www.osce.org/odihr/73461.

Open Society Justice Initiative. (2011). Written Comments in the Case of Yildirim v. Turkey. Retrieved from http://www.opensocietyfoundations.org/sites/default/files/echr-yildirim-written-comments-20110706.pdf.

Simon Wiesenthal Center. (2009). Facebook, YouTube+ : How Social Media Outlets Impact Digital Terrorism and Hate. Retrieved from http://www.wiesenthal.com/site/apps/nlnet/content2.aspx?c=lsKWLbPJLnF&b=4441467&ct=6994349#.UWV1WEqMrOk.

The United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information, Joint Declaration on Freedom of Expression and the Internet. (2011)