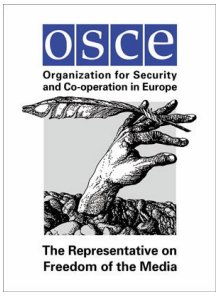

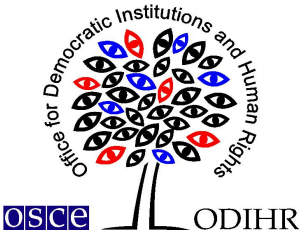

EXPERT WORKSHOP ON COMBATING THE USE OF THE INTERNET FOR TERRORIST PURPOSES

Issues Relating to Freedom of the Media, the Right to Freedom of Expression and the Right to Respect for Private Life and Data Protection

Contribution by

The Office of the Representative on Freedom of the Media (RFOM)

And

The Office for Democratic Institutions and Human Rights (ODIHR)

osce

Vienna, 13-14 October 2005

1. Introduction

The risk of terrorists and violent extremists using the Internet to further their purposes, whether through the dissemination of materials designed to encourage acts of terrorism, the transfer of funds through the Internet or through private communications in the planning and coordination of acts of terrorism is increasing as the use of the Internet becomes more widespread and efficient. This seminar is a timely one in focusing on the practicalities of combating the use of the Internet for terrorist purposes.

Interference with and monitoring of materials published on the World Wide Web or banking transfers or private correspondence conducted over the Internet do, however, entail a degree of interference with certain important rights relating, in particular, to private life, freedom of the media and freedom of expression. The OSCE in its multi-dimensional approach to security cannot afford to ignore these issues when considering the question of combating the use of the Internet for terrorist purposes. The Office of the High Representative on Freedom of the Media and the Office for Democratic Institutions and Human Rights have therefore drawn up a list of key principles that participating States and the OSCE should bear in mind in this context.

2. Basic Principles of Media Freedom

Governments are under various obligations by international law and conventions, including OSCE commitments safeguarding freedom of expression, when it comes to dealing, regulating or even interfering with the Internet.[i]

2.1. *General Principles*

- The Internet is an infrastructure combining different kinds of media (email, chat groups, World Wide Web etc.). It forms a public space and Internet media are protected under international law and media commitments to the same degree as traditional media.

- The Internet offers unprecedented means for people worldwide to distribute, exchange and access information. The positive aspects of the Internet outweigh the risks caused by the comparatively small amount of problematic content. Therefore any regulation must be applied carefully in order not to endanger the free flow of information.

2.2. *Regulation by Governments*

The essence and the value added of the Internet stem from the very fact that the Internet developed outside of any governmental regulation or interference. However, if governments do feel the need to regulate (parts of) the Internet as a measure to counter terrorism, the following safeguards should be applied**:**

- Combating the use of the internet for terrorist purposes must not be used as a pretext to curb the free flow of information. Prosecution of cyber-crime should only

target illegal activities and in no way affect the technical infrastructure of the Internet as such.

- No restriction on freedom of expression on the ground of national security or anti-terrorism may be imposed; unless the government can demonstrate that the restriction is prescribed by law and is necessary in a democratic society to protect a legitimate national security interest. The burden of demonstrating the validity and effectiveness of the restriction rests with the government.

- A clear distinction must be made between unwanted and illegal content as defined by law. Unwanted (or "harmful" or "problematic") content, though contested, deserves the full protection of the right of freedom of expression.

- If there is a need to take down illegal content from the Internet, this should happen according to the following principles:

  1. Internet content can only be declared illegal on the basis of a law and by a ruling of a court of justice.

  2. When it comes to regulating the Internet, there is a worrying tendency to shift responsibility to private operators, such as Internet Service Providers (ISP). RFOM feels that private bodies or companies are not appropriate instances to decide whether content is "legal" or "illegal".

  3. The procedure must be transparent and the right of appeal must be granted. The right to put any content back on the Internet, which was wrongly taken off, should also be observed.

  4. The principle of the "upload rule" must apply. All Internet content should be subject to the legislation of the country of its origin, not to the legislation of the country where it is downloaded.

2.3. *Filtering and blocking*

- Blocking or filtering of online content by governments is not in accordance with OSCE standards. In a democratic and open society it is up to the citizens/users to decide what they wish to access and view on the Internet.

- Any policy of filtering conflicts with the principle of free flow of information and might endanger the technical infrastructure of the Internet. Filters should only be installed by Internet users themselves. Such tools are commercially available and can be installed by users.

2.4. *Education*

- As with any risks or threats, education is a crucial element in reducing their negative effects. This is equally true for the risk of terrorist usage of the Internet. Especially among young Internet users, this educational potential has not been

exploited to its full extent. Education proves to be a better way of combating bad content than blocking or filtering. An educated mind is the best "filter".

- Education, media awareness activities and development of Internet literacy should be seen as the most effective way of combating bad content, including crime, hate speech or incitement to terrorist activities.

- The Internet also offers unique opportunities to promote tolerance and foster mutual understanding. This function of the Internet should not be forgotten in the discussion about illegal usage and criminal content.

3. Basic Principles on the Right to the Respect for Private Life and Data Protection

The right to private life, as enshrined in several human rights instruments, provides that every person has the right to be protected against unlawful interferences to her/his private and family life, home and correspondence.[ii] The use of Internet for communication purposes is also included.

3.1. *General Principles*

- The OSCE Human Dimension Commitments provide that "*The participating States reconfirm the right to the protection of private and family life, domicile, correspondence and electronic communications. In order to avoid any improper or arbitrary intrusion by the State in the realm of the individual, which would be harmful to any democratic society, the exercise of this right will be subject only to such restrictions as are prescribed by law and are consistent with internationally recognized human rights standards. In particular, the participating States will ensure that searches and seizures of persons and private premises and property will take place only in accordance with standards that are judicially enforceable*."[iii]

- The protection of one person's private life represents a challenging issue in the context of the fight against terrorism. In particular, since the Internet is used by terrorist organisations "*to identify and to recruit potential members, to collect and transfer funds, to organize terrorist acts, to incite terrorist acts in particular through the use of propaganda*,"[iv] States feel the need to exercise an effective control over the traffic of data circulating on the Web.

- The right to data protection is a very significant issue in democratic societies. Provisions concerning data protection may be found, at the European level, both in the Charter of Fundamental Rights of the European Union[v] and in well-established Council of Europe standards.[vi] Data protection issues are also dealt with in the EU, including in the framework of police and judicial cooperation.[vii]

- At present various governments[viii] are sponsoring reforms in national policies that require communications service providers (telephone companies and Internet Service Providers, mainly) to keep hold of their traffic data logs.[ix] Accordingly, the service providers would retain this information regarding users' e-mail, Internet and telephone use for periods of time one to five years long. The same trend has recently

emerged at the European Union level too.[x] The dilemma is where to strike a balance between legitimate security concerns and the right for citizens not to have their actions recorded for a number of years and available to government(s).

3.2. *Jurisprudence of the European Court of Human Rights*

- The expression "private life" must not be interpreted restrictively: it includes the right to establish and develop relationships with other human beings and also activities of a professional or business nature. Such a broad interpretation corresponds to existing Council of Europe's standards.[xi]

- According to art. 8 (2) ECHR, the right to private life may be limited by States in accordance with the law and if it is necessary in a democratic society 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 or morals, or for the protection of the rights and freedoms of others. These limitations must be narrowly interpreted.[xii]

- The existence of some legislation granting powers of secret surveillance over the mail, post and telecommunications is, under exceptional conditions, necessary in a democratic society in the interests of national security and/or for the prevention of disorder or crime.[xiii] The legislation at issue must be accessible and foreseeable as to its effects.[xiv]

- The law must indicate the degree of the discretion conferred on the competent authorities and the manner of its exercise with adequate precision. "Since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the legal discretion granted to the executive to be expressed in terms of an unfettered power."[xv]

- "[…] the Contracting States [do not] enjoy an unlimited discretion to subject persons within their jurisdiction to secret surveillance. The Court, being aware of the danger such a law poses of undermining or even destroying democracy on the ground of defending it, affirms that the Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate. The Court must be satisfied that, whatever system of surveillance is adopted, there exist adequate and effective guarantees against abuse. This assessment has only a relative character: it depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering such measures, the authorities competent to permit, carry out and supervise such measures, and the kind of remedy provided by the national law."[xvi]

- The mentioned safeguards should be established by the law concerning the supervision of the relevant services' activities. Supervision procedures must follow the values of a democratic society as faithfully as possible, in particular the rule of law, which is expressly referred to in the ECHR Preamble. The judiciary is in the best place to effectively check the interferences to the right to private life.[xvii]

- The storing of information relating to an individual's private life in a secret register and the release of such information come within the scope of the right to private life.[xviii] The fact that a public authority stores this information, makes use of it and refuses to allow an opportunity for it to be contested can amount to interference with the right to respect for private life secured in Article 8.1 of the ECHR.[xix]

4. Conclusion

The balance between different rights in the context of combating the use of the Internet for terrorist purposes is a complex question. A person cannot claim the protection of one right in order to act in breach of the rights of another. This paper seeks to set out certain basic principles from the OSCE Commitments and from international human rights law more broadly that may serve as a useful guide for those tasked with finding the correct point of balance. It is hoped that it will provide food for thought in this rapidly developing area.

The Office of the High Representative on Freedom of the Media and the Office of Democratic Institutions and Human Rights stand ready to assist participating States in the application of these principles and to further develop these complex questions.

Vienna, 13-14 October 2005

Paper presented jointly by the Office of the Representative on the Freedom of the Media and the Office for Democratic Institutions and Human Rights at the OSCE Expert Workshop on Combating the Use of the Internet for Terrorist Purposes

---

[i] More references may be found in OSCE Representative on Freedom of the Media, *The Media Freedom Internet Cookbook* (Vienna, 2004); OSCE Representative on Freedom of the Media, *Spreading the Word on the Internet* (Vienna, 2003); and also Joint declaration of the OSCE Representative on Freedom of the Media and Reporters Without Borders on Guaranteeing Media Freedom on the Internet (June 2005) and the Amsterdam recommendations on Freedom of the Media and the Internet (June 2003). These declarations and more background information on freedom of the Internet can be found on our website at www.osce.org/fom.

[ii] This is true both at universal and regional level: see, in particular, Article 17 of ICCPR and Article 8 ECHR.

[iii] Moscow 1991, para. 24.

[iv] OSCE Ministerial Council Decision No. 3/04, Sofia 2004.

[v] Article 8.

[vi] CoE Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981 and its Additional Protocol regarding Supervisory Authorities and Transborder Data Flows of 8 November 2001.

[vii] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector; concerning intergovernmental co-operation on criminal matters, see for instance the recent Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, MEMO/05/349, Brussels, 4 October 2005.

[viii] See for instance the UK Presidency Paper *Liberty and Security - Striking the Right Balance*, spec. pp. 4-10.

[ix] Traffic data include details about time, place and numbers used for fixed and mobile voice services, faxes, e-mails, SMS, and data on use of the internet. Subscriber (and sometimes user) data, such as the name and address of the subscriber, are also processed by providers or subscription-based electronic communications services.

[x] In this regard, see the European Commission's press release on the Draft *Data Retention Directive*, MEMO/05/328, Brussels, 21 September 2005.

[xi] This jurisprudence may be considered consolidated. See, among others, *Amann v Switzerland*, 16 February 2000, para. 65; and *Rotaru v Romania*, 4 May 2000, para. 43. In both cases the Court explicitely recalled the CoE Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data.

[xii] *Rotaru*, para. 47; in the same vein *Klass v Germany*, 6 September 1978, para. 42.

[xiii] *Klass*, para. 48.

[xiv] *Rotaru*, para. 52. See also *Silver and Others v UK*, 25 March 1983, para. 85-88; *Sunday Times*, para. 47; and *Malone v UK*, 2 August 1984, para. 67, reiterated in *Amann*, para. 50 and 56.

[xv] *Rotaru*, para. 55. The Human Rights Committee pointed out that "arbitrary interference can also extend to interference provided for under the law. The introduction of the concept of arbitrariness is intended to guarantee that even interference provided for by law should be in accordance with the provisions, aims and objectives of the Covenant and should be, in any event, reasonable in the particular circumstances," HRC General Comment No. 16: *The right to respect of privacy, family, home and correspondence, and protection of honour and reputation* (Art. 17 ICCPR), 08/04/88.

[xvi] See *Klass*, spec. para. 49 and 50, and para. 42. In the same vein, *Leander v. Sweden*, 26 March 1987, para. 60; *Malone*, para. 81; *Chahal v UK*, 15 November 1996, para. 131; and *Tinnelly & Son Ltd and McElduff v UK*, 10 July 1998, para. 77.

[xvii] *Klass*, para. 55.

[xviii] *Rotaru*, para. 43; *Leander*, para. 48.

[xix] *Kopp v Switzerland*, 25 March 1998, para. 53; *Rotaru*, para. 46; *Leander*, para. 48; and *Amann*, para. 69 and 80.