



## **EU-AT / EUROPOL**

### **CTTF2 Seminar on Islamist Extremist Activities on the Internet**

**The Hague, 28-29 March 2006**

#### **“PROTECTING HUMAN RIGHTS WHILE COMBATING THE USE OF THE INTERNET FOR TERRORIST PURPOSES”**

Background Paper by  
**The OSCE Office for Democratic Institutions and Human Rights  
(ODIHR)**

## Table of Content

1. Introduction .....	2
2. The Restriction of Rights and Freedoms in the Context of Fighting Terrorism – Some Preliminary Remarks .	3
2.1. Qualified Rights .....	3
2.2. Restricting Qualified Rights.....	4
a) <i>Is there a legal basis for the interference?</i> .....	4
b) <i>Is there a recognised ground for restricting rights?</i> .....	4
c) <i>Is it “necessary in a democratic society”?</i> .....	4
d) <i>Is it proportionate?</i> .....	4
e) <i>Is it discriminatory?</i> .....	5
3. Freedom of Speech .....	5
3.1. General Principles.....	5
3.2. Freedom of Speech and Regulating the Internet.....	7
4. The Right to Privacy and Data Protection .....	7
4.1. General Principles.....	8
4.2. Jurisprudence of the European Court of Human Rights .....	9
5. Conclusion.....	10

## 1. Introduction

The practice of terrorists and violent extremists using the Internet for propaganda, communication, recruitment and/or financing purposes is increasing as the use of the Internet becomes more widespread and efficient. It is obvious that governments have legitimate interests if not an obligation to take effective steps to counter and limit the impact of this activity. At the same time it is important to acknowledge that government interference with materials published on the Internet and monitoring of private online correspondence may engage human rights and fundamental freedoms as protected by domestic law and/or various (legally binding) international instruments. Rights that are particularly relevant in this context include the right to freedom of expression and the right to privacy.

The Organisation for Security and Co-operation in Europe (OSCE) has stood ready to tackle the challenges posed by the threat of international terrorism, including the issue of the use of the Internet for terrorist purposes. Its key commitments on combating terrorism are reflected, *inter alia*, in the OSCE Charter on Preventing and Combating Terrorism, the Porto Ministerial Council Decision No. 1 on implementing the OSCE commitments and activities on combating terrorism, the Bucharest Plan of Action for Combating Terrorism and the OSCE Strategy to Address Threats to Security and Stability in the Twenty-First Century.

In Decision No. 3/04, the OSCE Ministerial Council decided that participating States “exchange information on the use of the Internet for terrorist purposes and identify possible strategies to combat this threat, while ensuring respect for international human rights obligations and standards, including those concerning the rights to privacy and freedom of opinion and expression”.<sup>1</sup> This decision also tasked the Secretary General to organise, in co-operation with Interpol and other interested international organizations, an expert workshop to exchange information on the extent of this threat, as well as on the existing legal

---

<sup>1</sup> OSCE Ministerial Council Decision No. 3/04, “Combating the Use of the Internet for Terrorist Purposes”, Sofia, 7 December 2004.

framework and institutional tools, and to consider concrete measures to enhance international co-operation on this issue. This workshop was organised in Vienna on 13-14 October 2005.<sup>2</sup>

The aim of this paper is to outline some of the major human rights implications of the fight against terrorist use of the internet. In a first step, the paper will provide a brief and basic overview of how human rights work in practice, and under what circumstances those rights can be lawfully restricted. It will then focus specifically on the right to freedom of expression and the right to privacy. Taking into account general legal principles, decisions of the European Court of Human Rights as well as OSCE standards and commitments, it will try to outline basic guidelines that apply to the restriction of speech and privacy in the context of combating the use of the internet for terrorist purposes.

## **2. The Restriction of Rights and Freedoms in the Context of Fighting Terrorism – Some Preliminary Remarks**

States have legitimate and urgent reasons to take all due measures to eliminate terrorism. Acts and strategies of terrorism aim at the destruction of human rights, democracy, and the rule of law. They try to destabilise governments and undermine civil society. Governments therefore have a duty to protect their nationals and others against terrorist attacks and to bring the perpetrators of such acts to justice. At the same time it is imperative to ensure that measures taken to combat terrorism and violent extremism comply with obligations under international human rights law. Human rights law makes ample provision for counterterrorist action, even in the most exceptional circumstances, and it allows for the limitation and restriction of certain rights.

In order to understand how human rights work it is essential to recognise that different types of rights permit different types of interference with them. Therefore, it can be legitimate under certain circumstances to interfere lawfully with an individual's rights. Civil and political rights can be categorised into three different types of rights.

- Absolute rights permit no qualification or interference under any circumstances.
- Limited rights can be limited within the constraints spelt out within the Article itself.
- Qualified rights are intended to be balanced either between the individual on the one hand and the community on the other, or between two competing rights.

### **2.1. Qualified Rights**

The right to freedom of expression and the right to privacy are both qualified rights. Qualified rights are those rights where the right is asserted as a general principle – for example, the guarantee of freedom of expression – the relevant Articles then go on to qualify the right and to explain that it is lawful to interfere with it if it is necessary in a democratic society to do so and that there is a legal basis for such an interference. Therefore, it will be

---

<sup>2</sup> The gathering brought together 180 senior officials from 49 OSCE participating States and seven OSCE Partners for Co-operation, as well as international experts on the use of the Internet for terrorist purposes, along with representatives from 14 international organizations, including the G8, the Council of Europe, the Commonwealth of Independent States, the Organization of American States, the UN Office on Drugs and Crime, Interpol and the League of Arab States. See also <http://www.osce.org/atu/17702.html>.

lawful to place limitations on the right to freedom of expression, the right to private life, the right to protest and join trades unions, or the right to manifest religious belief.

It is almost self-evident that these rights can conflict with each other; the obvious example being that one person's right to private life may be another person's right to freedom of expression. A fair balance has to be struck between the two competing rights, and by understanding how to qualify rights lawfully it is possible to understand how civil and political rights work as a whole.

## **2.2. Restricting Qualified Rights**

Qualified rights can only be lawfully interfered with if the tests of legality, necessity, proportionality and non-discrimination have been satisfied.<sup>3</sup>

### *a) Is there a legal basis for the interference?*

What this means is that an individual must be able to know or find out what the law is that permits an interference with their Convention rights and they must be able to regulate their conduct in accordance with it.

### *b) Is there a recognised ground for restricting rights?*

The second test requires being able to justify the interference by reference to the recognised grounds for restricting rights within the Article itself. The State, therefore, has to be able to justify that the interference with the right is authorised by one or more of the stated grounds in the Article at issue.<sup>4</sup>

### *c) Is it "necessary in a democratic society"?*

The third test requires a balance to be struck between the rights of the individual on the one hand and State or community interests on the other. In order to make that assessment the government should justify its actions by making them establish that the interference is necessary in a democratic society. 'Necessary' does not mean indispensable, but neither does it mean 'reasonable' or 'desirable'.<sup>5</sup> What it implies is a pressing social need and that pressing social need must accord with the requirements of a democratic society. The essential hallmarks of such a society are tolerance and broad-mindedness.

Of particular relevance to counter-terrorism, although individual interests must on occasion be subordinated to those of the perceived majority, democracy does not simply mean that the views of the majority must always prevail: a balance must be achieved which ensures the fair and proper treatment of minorities and avoids any abuse of a dominant position.

### *d) Is it proportionate?*

The principle of proportionality is not mentioned in the text of human rights treaties, but it is the dominant theme in the application of human rights. What proportionality requires is that

---

<sup>3</sup> In the text of the ICCPR a number of Articles refer to limiting rights in different ways, such as if it is necessary in a democratic society or non-arbitrary. The test for both is ultimately the test of proportionality.

<sup>4</sup> See for example Article 19(3), ICCPR on Freedom of Expression which points out that, "It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary: (a) For respect of the rights or reputations of others; (b) For the protection of national security or of public order, or of public health or morals.

<sup>5</sup> *Sunday Times v United Kingdom* (Series A No 30), European Court of Human Rights (1979-80) 2 EHRR 245, 26 April 1979.

there is a reasonable relationship between the means employed and the aims sought to be achieved. Essentially proportionality requires a court to determine whether a measure of interference which is aimed at promoting a legitimate public policy is either:

- unacceptably broad in its application; or
- has imposed an excessive or unreasonable burden on certain individuals.<sup>6</sup>

A decision made taking into account proportionality principles should:

- impair as little as possible the right in question.
- be carefully designed to meet the objectives in question.
- not be arbitrary, unfair or based on irrational considerations.

Factors to consider when assessing whether or not an action is disproportionate are:

- Have relevant and sufficient reasons been advanced in support of it?
- Was there a less restrictive measure?
- Has there been some measure of procedural fairness in the decision making process?
- Do safeguards against abuse exist?
- Does the restriction in question destroy the “very essence” of the right in question?

*e) Is it discriminatory?*

As part of the test for assessing the legality of an interference with human rights, the issue of discrimination must be addressed, even if there has been no violation of the substantive right at issue. As a general principle, a distinction will be considered discriminatory if:

- it has no objective and reasonable justification;
- it does not have a very good reason for it;
- it is disproportionate.

If these criteria

cannot be fulfilled, and there is a difference of treatment, that difference of treatment will amount to discrimination and will be unlawful. In the counterterrorism context, particular attention has to be given to ensure measures are not adopted, and/or applied, which discriminate on grounds of race, religion, nationality or ethnicity.

### **3. Freedom of Speech**

#### **3.1. General Principles**

Article 10 of the ECHR reads as follows (see also the equivalent in the International Covenant on Civil and Political Rights [ICCPR], Article 19):

---

<sup>6</sup> In General Comment 31, the Human Rights Committee affirmed the notion of proportionality to the application and implementation of the ICCPR, adding that, “In no case may the limitations be applied or invoked in a manner that would impair the essence of a Covenant right”.

1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.

2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, 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.

The main elements of freedom of expression as guaranteed by international human rights law, include:

- Freedom of opinion
- Freedom of speech – orally, in writing, in print, in art
- Freedom of information – orally, in writing, in print, in art
- Freedom of the media
- Freedom of international communication

The European Court has consistently emphasised freedom of expression as one of the essential foundations of a democratic society and as one of the basic conditions for its progress and for “each individual’s self-fulfilment”. It is applicable not only to “information” or “ideas” that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that “offend, shock or disturb”.<sup>7</sup> At the same time, freedom of speech is not absolute. It is a qualified right, that “carries with it duties and responsibilities” and “may be subject to formalities, conditions, restrictions or penalties”.<sup>8</sup> (See Article 10 (2) ECHR)

As a general rule:

- Political speech in the context of terrorist activity can be limited;
- However, the extent of the limitation depends on the specific context and has to be determined on a case-by-case basis.
- Speech that falls short of incitement to hatred and incitement to violence is lawful, and further more, needs to be protected.

The highest protection is provided for criticism of governments and their policies. Public opinion expressed mainly through the media, must be free to scrutinise government actions. Governments, given their dominant position, must be prepared to accept criticism without resorting to criminal sanctions even if the criticism can be regarded as provocative or insulting or which involve serious allegations against security forces.

There is concern that authorities may use the fact of background political violence to create criminal offences in respect of political speech, particularly media reporting of banned

---

<sup>7</sup> See e.g. *Handyside v. UK* (7 December 1976, series A, no. 24) and *Fressoz & Roire v. France* ([GC], appl. No. 29183/95, para. 45).

<sup>8</sup> The most relevant cases are ECHR 13 September 2005, *İ.A. v. Turkey* (Appl. No. 42571/98) and ECHR 31 January 2006, *Giniewski v. France* (Appl. No. 64016/00). This case-law was developed from the earlier cases of *Otto Preminger v. Austria*, appl. No. 13470/87 (ECHR 1994) and *Wingrove v. UK* appl. No.17419/90 (ECHR November 1996).

organisations that, though provocative, insulting, offensive, shocking or disturbing, does not incite violence and should be protected.

The words in issue must be capable of being an incitement to violence and this matter, initially, can be addressed independently of context. The factor is whether violence, armed resistance or insurrection is encouraged. Words such as “resistance”, “struggle” or “liberation”, used approvingly, or accusations of “state terrorism” or “genocide” are in themselves insufficient to constitute incitement. The authorities may claim that words have a hidden or implicit meaning of support for violence. The European Court recognises this as a possibility but the burden is on the authorities to produce evidence of the double meaning.

### **3.2. Freedom of Speech and Regulating the Internet**

Governments are under various obligations by international law and conventions as well as OSCE commitments safeguarding freedom of expression, when it comes to dealing, regulating or even interfering with the Internet.<sup>9</sup> The essence and the value added of the Internet stem from the very fact that the Internet developed outside of governmental regulation or interference. However, if governments regulate (parts of) the Internet as a measure to counterterrorism, 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.
- Any restriction on freedom of expression on the ground of national security or anti-terrorism may be imposed must be justified by a demonstration 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 principle of the “upload rule”. 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.

## **4. The Right to Privacy and Data Protection**

---

<sup>9</sup> 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 at <http://www.osce.org/fom>.

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.<sup>10</sup> The use of Internet for communication purposes is also included.

#### 4.1. General Principles

Article 8 ECHR (see also Article 17 ICCPR) provides that:

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and 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.

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.”<sup>11</sup>

The right to data protection is a key component of the right to privacy. Provisions concerning data protection may be found, at the European level, both in the Charter of Fundamental Rights of the European Union<sup>12</sup> and in well-established Council of Europe standards.<sup>13</sup> Guideline V (*Collection and processing of personal data by any competent authority in the field of State security*) of the Council of Europe Guidelines on Human Rights and the Fight Against Terrorism, for example, states:

“Within the context of the fight against terrorism, the collection and the processing of personal data by any competent authority in the field of State security may interfere with the respect for private life only if such collection and processing, in particular:

- a) are governed by appropriate provisions of domestic law;
- b) are proportionate to the aim for which the collection and the processing were foreseen;
- c) may be subject to supervision by an external independent authority.”

Data protection issues are also dealt with in the EU, including in the framework of police and judicial cooperation.<sup>14</sup>

---

<sup>10</sup> This is true both at universal and regional level: see, in particular, Article 17 ICCPR and Article 8 ECHR.

<sup>11</sup> Moscow 1991, para. 24.

<sup>12</sup> Article 8.

<sup>13</sup> 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.

<sup>14</sup> 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



At present, various governments introduce reforms in national policies that require communications service providers (mainly telephone companies and Internet Service Providers) to keep hold of their traffic data logs.<sup>15</sup> Accordingly, the service providers would retain this information regarding users' e-mail, Internet and telephone use for a period of time of up to five years. The same trend has recently emerged at the European Union level, too.<sup>16</sup> The key question in this context is, of course, where to strike the balance between legitimate security concerns and the right of citizens not to have their actions recorded (and available to government) for a number of years.

#### 4.2. 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.<sup>17</sup> These limitations must be narrowly interpreted.<sup>18</sup> However, in accordance with Article 8 (2) ECHR the right to private life may be restricted.

The Court confirmed that 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.<sup>19</sup> However, the legislation at issue must be accessible and foreseeable as to its effects.<sup>20</sup>

In *Rotaru v Romania* the Court held that 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."<sup>21</sup>

The storing of information relating to an individual's private life in a secret register and the release of such information may violate the right to private life.<sup>22</sup> The fact that a public authority stores this information, makes use of it and refuses to allow an opportunity for it to

---

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.

<sup>15</sup> 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.

<sup>16</sup> In this regard, see the European Commission's press release on the Draft *Data Retention Directive*, MEMO/05/328, Brussels, 21 September 2005.

<sup>17</sup> This jurisprudence may be considered consolidated. See, *inter alia*, *Amann v Switzerland*, 16 February 2000, para. 65; and *Rotaru v Romania*, 4 May 2000, para. 43. In both cases the Court explicitly recalled the CoE Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data.

<sup>18</sup> *Rotaru*, para. 47; see also *Klass v Germany*, 6 September 1978, para. 42.

<sup>19</sup> *Rotaru*, para. 47; see also *Klass v Germany*, 6 September 1978, para. 42.

<sup>20</sup> *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.

<sup>21</sup> *Rotaru*, para. 55.

<sup>22</sup> *Rotaru*, para. 43; *Leander*, para. 48.

be contested, can amount to interference with the right to respect for private life as protected by Article 8 (1) of the ECHR.<sup>23</sup>

The Human Rights Committee – the UN treaty body monitoring the implementation of the ICCPR - has 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”.<sup>24</sup>

In *Klass v Germany* the Strasbourg Court held that “[...] 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.”<sup>25</sup>

The Court further held that 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 position to check effectively the interferences with the right to privacy.<sup>26</sup>

## 5. Conclusion

It is beyond question that government authorities have legitimate interests to combat terrorist use of the internet. At the same time, measures taken to counter this activity may infringe upon the right to freedom of speech and the right to privacy. The protection of these rights is of fundamental importance in a democratic society. Both the right to freedom of speech and the right to privacy are so-called qualified rights. They may thus be restricted under certain circumstances, including in the interests of national security. However, any restriction of these rights must be strictly lawful, necessary and proportionate. It is vital that while combating terrorism we do not unduly damage or destroy the very liberal democratic standards and values we are trying to protect and defend.

\*\*\*

---

<sup>23</sup> *Kopp v Switzerland*, 25 March 1998, para. 53; *Rotaru*, para. 46; *Leander*, para. 48; and *Amann*, para. 69 and 80.

<sup>24</sup> 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.

<sup>25</sup> 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.

<sup>26</sup> *Klass*, para. 55.