

# Ehtics and Human Rights in the Information Society

## Round table 4: Security and Governance

*The ethical issues concerning the protection of rights and freedoms of Internet users with regard to their actions and responsibilities*

## **The Interrelation of Human Rights and Security**

by Andreas Krisch  
<andreas.krisch@vibe.at>

### **About European Digital Rights**

European Digital Rights was founded in June 2002. Currently 28 privacy and civil rights organisations have EDRI membership. They are based or have offices in 17 different countries in Europe.

Members of European Digital Rights have joined forces to defend civil rights in the information society. The need for cooperation among organizations active in Europe is increasing as more regulation regarding the internet, copyright and privacy is originating from European institutions, or from International institutions with strong impact in Europe.

Some examples of regulations and developments that have the attention of European Digital Rights are data retention requirements, spam, telecommunications interception, copyright and fair use restrictions, the cybercrime treaty, rating, filtering and blocking of internet content and notice-and-takedown procedures of websites.

European Digital Rights takes an active interest in developments regarding these subjects in all 45 Member States of the Council of Europe.

Since January 2003, European Digital Rights produces EDRI-gram, a bi-weekly newsletter about digital civil rights in Europe.

### **Human Rights vs. Security**

For several years discussions and measures aiming for enhancing security and fighting terrorism claimed that it was a necessity to balance individual rights and security, implicating that the freedom of individuals opposes the needs of combating terrorism and law enforcement.

A report submitted by Europol provides figures on terrorism in the EU. According to the "TE-SAT 2007, EU Terrorism and Trend Report 2007"<sup>1</sup> a total of 498 attacks were carried out in 2006 in the EU, of which the vast majority were not intended to kill.

---

<sup>1</sup> "TE-SAT 2007, EU Terrorism and Trend Report 2007", Europol, March 2007, <http://cryptome.org/eu-terrorism.pdf>

“There were no successful Islamist terrorist attacks in the EU in 2006. However, a coordinated but ultimately failed attack aimed at mass casualties took place in Germany. The vast majority of terrorist attacks were perpetrated by separatist terrorist groups targeting France and Spain. In France, 283 attacks took place in Corsica in 2006. In Spain, despite the truce declared by ETA in March 2006, separatist groups perpetrated 136 attacks, mainly in the Basque region. Only the attack at the Madrid airport on 30 December 2006 resulted in casualties.”<sup>2</sup>

According to the report the remaining attacks were left- or right-wing-motivated or driven by other/not given motivation.

The number of arrested suspects differs from these figures. A total of 706 individuals suspected of terrorism offences were arrested, of which 257 arrested individuals were suspected of Islamist, 226 of separatist, 52 of left wing and 15 of right wing terror.<sup>3</sup>

With regard to the approximately 260 arrests related to Islamist terror “[l]ess than ten percent of the arrested individuals were suspected of preparation, planning or execution of terrorist attacks. [...] The vast majority of the arrested individuals were suspected of being members of a terrorist organisation. Other frequent criminal activities were financing of terrorism and facilitation.”<sup>4</sup>

The figures of the Europol report make clear that terrorism in the EU is mainly driven by separatists in France and Spain and focussing on Corsica and the Basque region. Of the relatively large number of arrests related to Islamic terror only less than 26 individuals were suspected of preparation, planning or execution of terrorist attacks.

On the other hand we had and still have to face a series of measures, limiting the freedom of individuals and infringing with human rights, arguing this to be necessary to fight terrorism.

Amongst these measures are not only

- the transmission of passenger name records (PNR) to the United States that approves the transmission of 19 pieces of data, including name, contact information, payment details, travel agency, itinerary and baggage information and allows to store the data for a time period up to 15 years<sup>5</sup>
- the access to financial data from SWIFT, allowing the United States a retention period of 5 years<sup>6</sup>
- the inclusion of biometric identifiers in EU passports, starting with a digital facial image stored on an RFID chip and soon to be complemented by fingerprints
- the agreement to mutually share information stored in police databases amongst EU members (Prüm treaty)<sup>7</sup> and
- the establishment of a central EU fingerprint database which is planned for 2008.<sup>8</sup>

<sup>2</sup> *ibid*, page 13.

<sup>3</sup> *ibid*, page 14.

<sup>4</sup> *ibid*, pages 19 – 20.

<sup>5</sup> Final agreements between EU and USA on PNR and SWIFT, <http://www.edri.org/edriagram/number5.13/eu-us-pnr-swift>

<sup>6</sup> *ibid*.

<sup>7</sup> From Schengen to Prüm: Data Protection under 3rd pillar a prerequisite,

<http://www.edri.org/edriagram/number5.4/prum>

Prüm's Treaty is now included into the EU legal framework, <http://www.edri.org/edriagram/number5.12/prum-treaty-eu>

<sup>8</sup> “Civil liberties threatened by the new centralized EU fingerprint database,

But also the directive on the mandatory retention of communication traffic and location data (2006/24/EG) is a measure fighting terrorism and organised crime. According to this directive traffic and location data of all communications of all 450 million Europeans, performed via telephone or via the Internet, have to be retained for a period of 6 months up to two years. This directive simultaneously revokes many of the safeguards in European human rights instruments, such as the Data Protection Directives and the European Convention on Human Rights.

Given the figures submitted by Europol it is questionable if the infringement of human rights and individual freedoms caused by this series of measures really is proportionate to the threat stemming from terrorism in Europe. Furthermore, it is questionable if this erosion of human rights standards in Europe is an adequate answer to terrorist attacks or if it might even be supportive to the aims of terrorists in destabilising our society by means of fear, uncertainty and doubt.

As the International Commission of Jurists stated in its Berlin Declaration:

„There is no conflict between the duty of states to protect the rights of persons threatened by terrorism and their responsibility to ensure that protecting security does not undermine other rights. On the contrary, safeguarding persons from terrorist acts and respecting human rights both form part of a seamless web of protection incumbent upon the state. Both contemporary human rights and humanitarian law allow states a reasonably wide margin of flexibility to combat terrorism without contravening human rights and humanitarian legal obligations.“<sup>9</sup>

In the “Statement on Human Rights, Human Dignity and the Information Society” elaborated and adopted by consensus by the participants of the International Symposium on the Information Society, Human Dignity and Human Rights in Geneva on 3-4 November 2003 it is elaborated with regard to privacy, that “[...] The use of increasingly invasive means of surveillance and of interception of communications, of intrusive profiling and identification and of biometric identification technology, the development of communication technologies with built-in surveillance capacities, the collection and misuse of genetic data, genetic testing, the growing invasion of privacy at the workplace and the weakening of data protection regimes give rise to serious concerns from the point of view of respect for human dignity and human rights.

[...]

It is fundamental to an understanding of the information society to recognize that information is power. Control of personal information and the deprivation of the right of privacy are ways of exercising power over individuals. The protection of personal information and privacy is central to the autonomy of the individual and to respect for human rights.

[...]

Certain measures taken in combating terrorism and cybercrime have eroded civil liberties and abrogated privacy rights. Cooperation in the field of criminal investigation must be accompanied by adequate enforcement of civil liberties and independent oversight of data collection.”<sup>10</sup>

---

<sup>9</sup> <http://www.edri.org/edriagram/number5.6/fingerprint-database-eu>

<sup>9</sup> The Berlin Declaration, The ICJ Declaration on Upholding Human Rights and the Rule of Law in Combating Terrorism, International Commission of Jurists, 28.08.2004, [http://www.icj.org/IMG/pdf/Berlin\\_Declaration.pdf](http://www.icj.org/IMG/pdf/Berlin_Declaration.pdf)

<sup>10</sup> Statement on Human Rights, Human Dignity and the Information Society, International Symposium on the Information Society, Human Dignity and Human Rights, Palais des Nations, Geneva, 3-4 November 2003 <http://www.pdhre.org/wsis/statement.doc>

# Cybercrime

Not only measures taken to support the so-called fight against terrorism impact the freedom of individuals and privacy, but also the Council of Europe Convention on Cybercrime lacks protections of privacy and civil liberties.

Starting in 2000, when the first draft of the Convention was made public (v.19) the Global Internet Liberty Campaign (members of which founded EDRi in 2002) articulated their deep concerns regarding this Convention in two letters to the Council of Europe and published in November 2001, after the Convention was signed “Eight Reasons the International Cybercrime Treaty Should be Rejected”<sup>11</sup>

These eight reasons are:

- **Reason #1: Lack of Privacy and Civil Liberties Protections**  
There is no provision to protect citizens privacy, only vague references in the preamble.
- **Reason #2: A far too broad Convention**  
Through its procedural provisions the Convention covers any crime where evidence could be in computerized form, but computers are everywhere in modern life.
- **Reason #3: No Dual Criminality Requirement for International Cooperation**  
Law enforcement Agencies of a given country could find themselves forced to cooperate in investigations of behavior illegal in another country, but legal within its borders. This could lead to surveillance of citizens who committed no crime under their own laws. Mutual assistance requests may come from countries with minimal civil liberties protection. This danger is growing with current activities to actively encourage further countries to sign the convention.
- **Reason #4: Protection of Political Activities too Weak**  
A consequence of the missing dual criminality requirement: The use of the Convention to force one country to cooperate in politically inspired investigations by another. The exceptions allowing to refuse cooperation in such cases are limited and not included in all provisions. A definition of „political offenses“ is missing. In some provisions no judicial approval or oversight is needed for authorization of official assistance (art.27-2.b): A law enforcement agency could solely decide that an offense is not political and start surveillance.
- **Reason #5: Further Unbalance of Intellectual Property Laws Allowed**  
Copyright infringements are criminalized without any mention of counterbalancing rights (fair use, parodies criticisms,...)
- **Reason #6: Police given invasive new surveillance powers**  
The Convention allows for systems for direct access of ISPs and telecom operators networks.
- **Reason #7: Broad criminalization of hacking tools**  
Criminalization of tools rather than behaviors.
- **Reason #8: A Convention Drafted in a Closed and Secretive Manner**  
A non democratic process: No inclusion of public interest groups, mainly law

---

<sup>11</sup> Eight Reasons the International Cybercrime Treaty Should be Rejected, GILC, <http://www.treatywatch.org/about.html>

enforcement authorities. Little efforts to include concerns of privacy and civil liberties groups. Lack of balance with adequate safeguards to enforce human rights and the rule of law.

Before any further extension of the Convention in scope and/or ratification/accession, an assessment of the Convention and its national implementations with regards to human rights, democracy and the rule of law should be undertaken. Furthermore, an equivalent energy should be devoted to extend ratifications/accessions to Convention n°108: Protection of Individuals with regard to automatic processing of Personal data (1981).

## **An Information Society for All**

Given the series of measures for fighting terrorism and crime, limiting the freedom of individuals and infringing with human rights, it is necessary to reconsider their impact on human rights, which are the foundation of our society, and to rediscover the protection of human rights as a core obligation of all European states.

To this end a multi stakeholder approach should be taken, involving all relevant groups, governments, private sector and civil society alike. First steps have already been taken during the World Summit on the Information Society. The Internet Governance Forum (IGF) was a further step forward in terms of participation and in terms of setting the substantive agenda. The concrete outcome of the IGF will depend on how seriously it is treated and if the results elaborated by this forum will find their way into binding policy.