Strasbourg, 4 December 2008
CommDH/IssuePaper(2008)3

Protecting the right to privacy in the fight against terrorism
by Thomas Hammarberg, the Commissioner for Human Rights

CONTENTS

Commissioner's Issue Papers
Issue Papers are commissioned and published by the Commissioner for Human Rights for the purpose of contributing to debate or further reflection on a current and important human rights matter. All opinions in these expert papers do not necessarily reflect the position of the Commissioner. The Issue Papers are available on the Commissioner's web-site: www.commissioner.coe.int.

Acknowledgements

The Commissioner for Human Rights expresses his thanks to Professor Douwe Korff, of London Metropolitan University, for his assistance in preparing this paper as an external consultant for the Office.

1. Introduction

The right to privacy is an integral part of the right to respect for private life, as guaranteed by Article 8 of the European Convention on Human Rights: it also encompasses a more special right, usually referred to in terms of "data protection". This special right does not only concern protecting individuals from intrusions into their privacy or private life, but also more broadly is about guarding against the improper collecting, storing, sharing and use of their data. It addresses the central issue in the "information society" of the extent of control by data controllers over individuals –tellingly referred to as "data subjects" - through possession of their data. The increasing importance given to this right is reflected in the case-law of both the European Court of Human Rights and the European Court of Justice.

In spite of the great attention given to terrorism, especially after "9/11", a precise definition of terrorism has still not been universally agreed upon. This is perhaps because universal consensus cannot be reached on what constitutes a terrorist and what a freedom fighter. The EU has said that 'terrorism', comprises:

"[the threat or act of] seriously intimidating a population, unduly compelling a Government or international organisation to perform or abstain from performing any act, or seriously destabilising or destroying the fundamental political, constitutional, economic or social structures of a country or an international organisation" (Framework Decision 2002/475/JHA, Article 1)

Yet, neither the 1977 (COE) European Convention on the Suppression of Terrorism, nor the 1999 UN International Convention for the Suppression of Terrorist Bombings defines the word "terrorism". Nor has the UN Security Council adopted a definition, despite the fact that it mandates punitive actions against (suspected) "terrorists".

The issues addressed in this paper are therefore placed in a highly sensitive, yet ill-defined context. They touch, on the one hand, fundamental values of a democratic society, raising serious constitutional questions in many States. On the other hand, they relate to a phenomenon - terrorism - in response to which States feel entitled, even obliged, to take the most drastic action.

Terrorism, however defined, is not a passing phenomenon. While wars or other public emergencies generally have a more or less clear end (even if this can be much delayed), there is no end in sight to the fight against global terrorism. Even at the national level, anti-terrorism legislation tends to become semi-permanent.

Terrorism, and measures against terrorism, therefore pose a long-term, engrained threat to the fundamental values of the Council of Europe and its Member States. One particular area at risk concerns the collection, storage, analysis, sharing and use of personal data. Data protection is often seen as an obstacle to effective anti-terrorist measures - and thus as a prime area in which basic international commitments are ignored. Yet data protection is crucial to the upholding of fundamental democratic values. It is this tension between strong opposing forces, the desire to prevent terrorism and the importance of protecting human rights, that makes this a matter of pressing concern.

The Council of Europe and the European Union have recently agreed to promote their co-operation, *inter alia*, in relation to "*combating terrorism, organised crime, corruption, money laundering and other modern challenges, including those arising from the development of new technologies*."[1] The Commissioner for Human Rights is among those who are "especially

invited" to participate in this enhanced cooperation.[2] Human rights issues arising from policies relating to privacy and the fight against terrorism, and indeed from more general policies on information technologies, are therefore of interest to him.

2. Technological developments

Technological developments have a close bearing on responses to terrorism and come in several increasingly inter-related forms. First, there are new technologies of direct surveillance: high-definition, wi-fi broadband-enabled CCTV, combined with face (and gait) recognition software; motorway cameras that can read car licence plates and track selected cars; technologies to monitor, screen and analyse billions of telephone and email communications simultaneously, in real time; virtually undetectable "bugs" and tracing technologies; and "spyware", surreptitiously installed on a suspect's personal computer by the authorities, that can remotely, and secretly, monitor all the suspect's online activities and emails, obtain his or her passwords, and even turn on the computer's camera and microphone.

These systems no longer just watch: companies and governments have developed, or are developing, software that supposedly identifies "suspicious behaviour" and even whether a person has "hostile intent". Surveillance computers don't just survey: they direct the attention of police and other authorities to specific "targets".

Secondly, there is a massive expansion in "dataveillance": the monitoring of the "data trails" left by individuals in numerous transactions, through access to private and public-sector databases. The former include commercial databases, such as company customer records, communication data etc. Some are in the semi-public sector. In several countries, fingerprints (or hand contours) are used for access-control to libraries and school canteens. In addition, States are creating ever more powerful central databases of their own, with biometrics such as computer-readable facial photographs, fingerprints, DNA, etc. In the UK, DNA is taken from everyone who is arrested, and retained even if they are exonerated of the crime in question. In many countries, there are central databases holding social security, pension and benefit details; in an increasing number there are central databases with medical records on large sections of the population; yet others contain all details of contacts with the police (whether as a suspect, victim or witness). The citizen has no choice in the provision of such data, and such compulsion is increasingly internationalised. Thus, EC Regulation 2252/2004/EC mandates the collection and retention of fingerprints from all EU passport holders - i.e. hundreds of millions of innocent European citizens. Data on airline travellers is similarly compulsorily obtained, analysed and used for anti-terrorist purposes.

Combining these databases, and linking them with other databases – such as consumer "lifestyle" databases built by specialised data mining companies, or credit reference agencies, or travel agents – creates a previously unimaginably detailed picture of our lives and interests, cultural, religious and political affiliations, financial, and medical aspects. Yet the data protection safeguards against the transferring of information are weak - and further weakened by anti-terrorist legislation. The individual stands increasingly naked before the national and international authorities.

Thirdly, the police and secret services search through such databases in order to find a "match" against a pre-determined (but dynamically updated) "profile". Moreover, such searches are increasingly: (a) "intelligence-led"; and (b) carried out as part of European (rather than just national) policies.

Many of these technologies clearly pose inherent threats to our privacy and freedoms: they allow the State to monitor our lives at a close level. But they are not infallible. On the contrary, these technologies are subject to serious limitations and even built-in biases. Parliamentary committees, civil liberties groups, opposition members of Parliament and others who would challenge the arrangements between authorities and high-tech industry are often not equipped to do so: they do not fully understand the technical details or implications (and are often denied access to the technical details, "to protect commercial secrecy"). The more high-tech a product, the more difficult it is to assess its claims, and weaknesses.

Technologies which enable "profiling" and "data mining", may seem to work up to a point, but inevitably lead to actions against large numbers of innocent people, on a scale that is both unacceptable in a democratic society and renders the "trawl" useless. It is important to stress the inevitability in this: this is not something that can be fixed by better design. Attempts to identify very rare incidents or targets from a very large data set are mathematically certain to result in either an unacceptably high numbers of "false positives" (identifying innocent people as suspects) or an unacceptably low number of "false negatives" (not identifying real criminals or terrorists). As a very recent, authoritative study by the US' National Research Council (the US National Academies) concluded:

Automated identification of terrorists through data mining (or any other known methodology) is neither feasible as an objective nor desirable as a goal of technology development efforts. [3]

3. Enhanced police co-operation

In Europe, the police are increasingly seen as part of a wider "full societal alliance", implementing overall State policies. The emphasis is more and more on prevention, and on joining criminal justice/police action with other, wider social policy approaches.

This "societal alliance" approach requires much-increased data sharing between the police and other State bodies, such as social services and educational establishments. Undoubtedly, there are clear benefits to such "joined-up" policies and to the coordination of the work of different agencies. However, there is a danger that these data-collecting and sharing arrangements could lead to an almost complete surveillance culture.

A further major change in the policing environment concerns the relationship between the police and the secret services in a number of countries. Apart from obtaining information through the advanced surveillance and "dataveillance" technologies mentioned earlier, or receiving it from the secret services, information is also obtained through undercover

agents and informants. As a result, the basis for police (and others') "interest" in a person, and the nature of the evidence against that person, are increasingly hidden. This has a direct impact on the treatment of such a person, who might be spied upon, harassed, arrested, denied a job or a research post[4] - all without knowing why, or able to challenge the reasons for such actions (or without even being aware of it). The increasingly close relationship between the police and the secret services also has the potential to undermine the fairness of trials against persons accused of being involved in organised crime or terrorism, in that courts increasingly allow effectively secret evidence and evidence from anonymous witnesses to form the basis for a conviction.[5]

4. The legal framework

The legal framework defining the right to privacy in the context of the fight against terrorism is complex. The law is developed under a range of separate instruments at the national and International level.

At the most general level, data protection has been developed on the basis of Article 8 of the European Convention on Human Rights.[6] In the last few years, the European Court of Human Rights has given strong recognition to data protection principles under this article, in particular in the cases of *Peck v. the UK* (concerning CCTV), *Amann v. Switzerland* (concerning telephone interception) and *Rotaru v. Romania* (concerning secret service files).[7] See also the recent case of *Copland v. the UK* (concerning the question of when the legal basis for processing of personal data can be considered to be adequate, i.e. when it can be said to constitute "law" in terms of the ECHR).[8]

Data protection is, however, also increasingly seen as a *sui generis* right, in particular in the EU Charter of Fundamental Rights, where it is given a separate provision (Article 8).[9] More specifically, the following general European data protection instruments have been developed:

· the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and its Additional Protocol;[10]

· Directive 95/46/EC of the European Parliament and 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;[11] 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 (also referred to as the e-Privacy Directive).[12]

> [Note: (i) this directive is subsidiary to Directive 95/46/EC; and (ii) it has been amended to allow for the mandatory retention of communications data by communication service providers, for the benefit of law enforcement.][13]

Under these instruments, rules and guidelines have been issued that specifically relate to processing of personal data for law enforcement purposes. These include, in particular, CoE Recommendation R(87)15 of the Committee of Ministers to Member States, Regulating the Use of Personal Data in the Police Sector (1987).[14] This recommendation has become the effective standard on the issue: it is expressly referred to in various European police co-operation instruments, including the Schengen and Europol treaties and associated regulations, and is also regularly invoked in recommendations by the Parliamentary Assembly of the Council of Europe and its Committee of Ministers, as well as by the European Parliament.

The European Court of Justice in Luxembourg, like the Strasbourg Court, has also been quite strict in its application of data protection principles (in the case of the ECJ, derived from both the ECHR as reflected in "general principles of Community law" and from the above EC directives; see in particular the cases of *Österreichischer Rundfunk v. Austria* and *Lindqvist v. Sweden*).[15] Importantly, it is clear from these cases that in the view of the European Court of Justice, data protection is a fundamental, constitutional issue: the principles of the main Data Protection Directive must be construed as fundamental, constitutional human rights principles, and applied in accordance with the case-law of the European Court of Human Rights. More specifically, the ECJ has clearly endorsed, and adopted for itself, the typical, "standard" approach to human rights developed by the Strasbourg Court - and follows this approach also and in particular in its assessment of cases relating to the Framework Directive.

The following broad standards can be derived from the judgments of the European Court of Human Rights, and are reflected in the case-law of the European Court of Justice, and in Recommendation R(87)15:

> 1. There must be a legal basis for any collection, storing, use, analysis, disclosure/sharing of personal data for law enforcement and anti-terrorist purposes. A vague, broad general statutory basis is not sufficient;[16] rather:
>
> 2. Such processing must be based on specific legal rules relating to the particular kind of processing operation in question; these rules must be binding, and they must lay down appropriate limits on the statutory powers such as:
>
> - o a precise description of the kind of information that may be recorded;
> - o a precise description of the categories of people against whom surveillance measures such as gathering and keeping information may be taken[17]
> - o a precise description of the circumstances in which such measures may be taken
> - o a clearly set out procedure to be followed for the authorisation of such measures;
> - o limits on the storing of old information and on the time for which new information can be retained;

o explicit, detailed provisions concerning:

- the grounds on which files can be opened;
- the procedure to be followed [for opening or accessing the files];
- the persons authorised to consult the files;
- the nature of the files;
- the use that may be made of the information in the files.

It follows from the above:
(1) that the collection of data on "contacts and associates" (i.e. on persons not suspected of involvement in a specific crime or of posing a threat), the collection of information through intrusive, secret means (telephone tapping and email interception etc.; "bugging"; informers; agents), and the use of "profiling" techniques, and indeed "preventive" policing generally, must be subject to a particularly strict "necessity" and "proportionality" test (and surrounded with particularly strong safeguards: see below);

(2) that "hard" (factual) and "soft" (intelligence) data should be clearly distinguished; and that data on different categories of data subjects (officially indicted persons, suspects, associates, incidental contacts, witnesses and victims, etc.) should likewise be clearly distinguished;
(3) that the nature of information and intelligence coming from private parties such as businesses or credit reference agencies requires additional safeguards, *inter alia* in order to ensure the accuracy of this information since these are personal data that have been collected for commercial purposes in a commercial environment; and
(4) that access should only be allowed on a case-by-case basis, for specified purposes and under judicial control in the Member States.

3. Such rules can be set out in subsidiary rules or regulations - but in order to qualify as "law" in Convention terms, they must be published.

4. In order to comply properly with the core "purpose-specification and limitation" principle, the following rules should be complied with:

o it is important to be as precise as possible; it is not sufficient to specify that processing serves "the police task", or even a specific police task (investigation and prosecution of crime; countering immediate threats; more controversially, "prevention");

o personal data, collected for one specific police purpose (e.g. countering threats) can only be used for another specific purpose (e.g. investigating offences) if the data could have been independently collected for that second purpose;

o personal data should never be collected by the police or other law enforcement agencies "just in case".

5. "*The collection of data on individuals solely on the basis that they have a particular racial origin, particular religious convictions, sexual behaviour or political opinions or belong to particular movements or organisations which are not proscribed by law should be prohibited. The collection of data concerning these factors may only be carried out if absolutely necessary for the purposes of a particular inquiry.*" (Principle 2.4 of Recommendation R(87)15)

6. EC Directive 95/46/EC stipulates, for the First Pillar, that if a person is subjected to a fully-automated decision, the individual should (at least) have the right to know the logic involved in this decision, and measures should be taken to safeguard the individual's legitimate interest. The scope and application of this principle is still rather unclear, even in the First Pillar. However, the underlying principle - that it would violate human identity, dignity or personality to treat anyone on that basis without stringent safeguards - must surely also be applied in the Third Pillar. This clearly has implications for the kind of "profiling" of terrorist suspects, discussed earlier.

7. In addition, there must be strong "safeguards established by law" which ensure "appropriate [and effective] supervision of the relevant services' activities". This supervision should "normally" be carried out by the judiciary. If it is not, there should be particularly strong alternative supervisory mechanisms, such as close Parliamentary scrutiny.[18] The latter, procedural (supervision) requirement is part of the test of whether the legal rule in question has the appropriate quality. But the existence of such procedures is also essential in the assessment of compliance with Article 13 ECHR (the right to an effective remedy before a national authority). The European Court of Human Rights also confirmed that a remedy should be available to anyone with an "arguable claim" of a violation of a Convention right: there is no need to show that an actual violation has occurred - which in the case of secret surveillance would put individuals in an impossible position.

5. The European context

The issues addressed in this paper have to be placed in a complex international-institutional framework. They relate to activities by the United Nations Security Council, the Organisation for Security and Cooperation in Europe (OSCE), various political and policy- making bodies of the Council of Europe (for example, the Parliamentary Assembly, the Committee of Ministers), different organs of the European Union (the European Parliament, the European Commission, with the European Council dominating), NATO, and major countries, in particular the USA. Depending on the actor (or the organ), they relate to political, diplomatic, police, intelligence and military matters.

The fight against terrorism is increasingly seen as a global problem which requires a global response. On the one hand, the legal bedrock of human rights and data protection is provided at the European level. On the other hand, policies that may

challenge these very same European human rights standards, such as counter-terrorism policies, are also being created at a European level. Accordingly, the following section will focus on European Union policy action in the fight against terrorism and organised crime, and look at how it intersects with data protection issues.

5.1 Promotion of information technologies

The European Union strongly encourages the use of new IT technologies in areas such as e-government, e-health, e-inclusion, e-learning, etc, as well as the provision of pan-European e-services by the (increasingly global) private sector. Similar policies encouraging more use of information technologies are evident in relation to law enforcement - with counter-terrorism acting as a powerful catalyst.

The European Commission considers electronic identification management (eIDM) to be among the "critical key enablers" of e-government:[19]:

Biometric national ID cards and eIDM for public services are markedly different: national ID cards serve public security, for example by facilitating integrated border management and supporting the fight against terrorism, whereas electronic identification for public services is intended to ease access and offer personalised and smarter services. [20]

In data protection terms, this should make it imperative to separate ID cards from eIDM products, and to isolate the databases behind these different products.

5.2 EU law enforcement systems and databases

Europol

Europol is the European Union law enforcement organisation that handles criminal intelligence. Its aim is to improve the effectiveness of and co-operation between the competent authorities of the Member States in preventing and combating serious international organised crime and terrorism. Its mission is to make a significant contribution to the European Union's law enforcement action against organised crime and terrorism with an emphasis on targeting criminal organisations. The European Council wants to "*strengthen[ ] Europol's operational capabilities.*"[21]

Eurojust

Eurojust was established in 2002 as the first permanent international network of criminal-judicial authorities created anywhere in the world.[22] It "*stimulates and improves the co-ordination of investigations and prosecutions between competent authorities in the Member States ... in particular by facilitating the execution of international mutual legal assistance and the implementation of extradition requests.*" It also "*hosts meetings, with translation facilities, between investigators and prosecutors from different states dealing with individual cases and at a strategic level and specific types of criminality.*" Its work increasingly covers terrorist cases, and it would like to expand this.[23]

Eurodac

Eurodac is a system that allows for the cross-checking of fingerprints on asylum seekers and suspected illegal migrants, and thus helps the effective application of the Dublin convention on handling claims for asylum. The main concern for the present paper is that under new proposals, and in particular under the new principle of "availability", the use and purposes of the Eurodac database will be extended to basically all matters relating to law enforcement and public security in the EU, including terrorism. The Standing Committee of Experts on International Immigration, Refugee and Criminal law (the "Meyers Committee") strongly objected to this in a letter, stressing that:

EU measures or policies in the field of Freedom, Security, and Justice should not be based on the general presumption that migrants within the EU are to be treated as suspected terrorists. Such a policy would run against the general accepted principles in EU law of non-discrimination and equality. It is also devastative for the position of migrants and their further integration into the society of EU Member States. [24]

Schengen Information System (SIS)

The Schengen Information System (SIS) was originally a measure to counter the risks stemming from open borders, with limited data. However, following extension under what is now known as SIS-I+, plans are well-advanced for an updated system, SIS-II. This new system is to have "*more advanced functionalities*" and will be based on "*cutting-edge technology*." With the new system, it should also be possible "*to connect other Member States*."[25] It will contain lists of all individuals who are to be denied entry, as well as lists of people classified as "known" or "suspect" in relation to crime and terrorism, and another list covering those to be placed under surveillance. Access is to be extended to Europol, Eurojust, national prosecutors and vehicle licensing authorities.

As the UK House of Lords noted, SIS-II will thus store "*an enormous volume of sensitive personal data*."[26] More generally, as the European Commission acknowledged, the functions of the SIS will be transformed "*from a reporting system to a reporting and investigation system*".[27] Yet as the House of Lords also noted, "*the data protection regime applicable to the SIS-II rules is unduly complex*."

Visa Information System (VIS)

The Visa Information System (VIS) was established in 2004 as a system for the exchange of visa data between Member States. During a meeting of the Council of the European Union on 7 March 2005, it was concluded that 'in order to achieve fully the aim of improving internal security and the fight against terrorism' Member State authorities responsible for internal security should be guaranteed access to the VIS. In July 2007, "*the [European] Council called for swift implementation of [its] decision on access by police authorities (including Europol) to the VIS database for prevention, detection and investigation of terrorist offences.*"[28] Such access was agreed by a Council Decision on 23 June 2008.[29]

Customs Information Systems (CIS)

This is a first and third pillar database set up to help customs and related authorities prevent, investigate and prosecute serious contravention of national laws. Information may be recorded for the purpose of sighting and reporting, discreet surveillance or specific checks. CIS is managed by OLAF, the European Anti-Fraud Office, in cooperation with the European Commission's Justice and Home Affairs DG and the Taxation and Customs Union DG.

Although mainly active in relation to customs fraud, CIS data can also relate to terrorism, e.g., in relation to money-laundering, drug-smuggling or other "ordinary" fraud or customs crimes perpetrated to support terrorism.

The Prüm Treaty

On 27 May 2005 the Prüm Treaty was signed by Germany, Spain, France, Luxembourg, Netherlands, Austria and Belgium. It covers a series of justice and home affairs issues including the [free] "exchange of information". For example, Articles 2 – 12 allow direct access by the law enforcement agencies in the participating states to each other's databases on DNA, fingerprints and vehicle registration, on a "hit/no-hit" basis. If there is a "hit" the file is provided. Indeed, the Treaty requires the establishment, in the State Parties, of certain databases, including a DNA database, and imposes a duty on State Parties to obtain DNA from "particular individual[s]" (not necessarily suspects) if no DNA is available in the national database. Terrorism is explicitly included in the remit.

By its Decision of 23 June 2008[30] the European Council agreed to integrate the main provisions of the Prüm Convention into the EU's legal framework, to enable wider exchanges (between all EU Member States) of biometric data (DNA and fingerprints) in the fight against terrorism and cross border crime. All EU Member States will therefore be required to set up DNA databases.

5.3 The principle of "availability"

The principle of "availability" was defined in the 2004 "Hague Programme" of the European Union as follows:[31]

With effect from 1 January 2008 the exchange of ... information should be governed by conditions set out below with regard to the principle of availability, which means that, throughout the [European] Union, a law enforcement officer in one Member State who needs information in order to perform his duties can obtain this from another Member State and that the law enforcement agency in the other Member State which holds this information will make it available for the stated purpose, taking into account the requirement of ongoing investigations in that State.

The methods of exchange of information should make full use of new technology and must be adapted to each type of information, where appropriate, through reciprocal access to or interoperability of national databases, or direct (on-line) access, including for Europol, to existing central EU databases, such as the SIS.

In effect, this gives the national law enforcement agencies within the EU full access to all the data in all national and European databases. In particular, the aim is to allow such data sharing and free access without any of the usual "obstacles", contained in the traditional instruments for transnational cooperation between law enforcement agencies - such as the 1959 (Council of Europe) European Convention on Mutual Assistance in Criminal Matters (ETS 030) and its two additional protocols and the EU Convention on Mutual Assistance in Criminal Matters between the Member States of 2000 (which built on the CoE Convention), with its accompanying Protocol (2001), which both came into effect in 2005. The procedures under these treaties take time and, more importantly, involve formal requests for specified information and, in many cases, require judicial authorisation.

In fact, these "obstacles" in many cases constitute fundamental safeguards for the individual. As the European data protection authorities put it in their statement from their meeting in Cyprus in May 2007:

In view of the increasing use of availability of information as a concept for improving the fight against serious crime and the use of this concept both on a national level and between Member States, the lack of a harmonised and high level of data protection regime in the Union creates a situation in which the fundamental right of protection of personal data is not sufficiently guaranteed anymore.

The DPAs suggested that a "comprehensive framework" be developed for reliance on the "availability" principle, and set out a series of guidelines and principles in this respect. Application of these would considerably limit the use of the principle, and provide for safeguards.[32]

While the proposal for the formal adoption of the availability principle has been withdrawn, the principle still remains the

underpinning on data exchanges, for example in the Prüm Treaty.

5.4 The draft EU Council Framework Decision on the Protection of Personal Data

The proposed EU Council Framework Decision on the protection of personal data in the framework of police and judicial co-operation in criminal matters aims to ensure a high level of data protection throughout the Third Pillar. However, it has been severely criticised by the European Parliament, the European Data Protection Supervisor (EDPS), all the European data protection authorities, and by civil society and a number of human rights groups. Overall, critics are of the opinion that the proposal as currently drafted encourages, in the EU "Third Pillar" area, a trend towards the lowest common data protection denominator. Critics voice the opinion that the current proposal falls short of established European standards - in particular the CoE data protection convention (Convention No. 108), the recommendation on police data adopted under it (Recommendation R(87)15, already mentioned), and more broadly and fundamentally, Article 8 of the European Convention on Human Rights. The draft Decision also appears to create loopholes through which strict data protection rules in some EU countries could be circumvented by "routing" data through other countries, in which there are less restrictions. On top of this, the activities of the secret services and the police in relation to national security are to be excluded from the Decision and, thus, from any effective data protection guarantees.

5.5 Passenger Name Record data or PNRs

Passenger Name Record data (PNRs) are related to travel movements, usually flights, and include passport data, name, address, telephone numbers, travel agent, credit card number, history of changes in the flight schedule, seat preferences and other information. Air carriers already capture the PNR data of passengers for their own commercial purposes, however, only a limited number of European states have adopted legislation to set up mechanisms to oblige air carriers to provide the relevant PNR data and to have such data analysed by their authorities.

Air carriers already communicate some form of data to the authorities of EU Member States, namely Advanced Passenger Information (API)[33] which principally relates to border control and the fight against illegal immigration. PNR data contains more data elements than API data, which is simply official data from passports. According to the European Commission, PNR is of more interest in the fight against terrorism because 'such data elements are a very important tool for carrying out risk assessments of the persons, for obtaining intelligence and for making associations between known and unknown people.'[34]

Agreements for the transmission of PNR data in the context of the fight against terrorism and transnational organised crime have been concluded between the EU and the United States[35], Canada and recently Australia[36].

In 2004, the European Counil invited the Commission to bring forward a proposal for a common EU approach to the use of passengers' data for law enforcement purposes. The European Union's Proposal for a Council Framework Decision on the use of Passenger Name Record for law enforcement purposes was presented by the Commission in November 2007, after a period of consultation with relevant stakeholders.

A number of significant reservations have been voiced regarding this Proposal from the Article 29 Working Party[37] and civil society. In his Opinion on the Draft Proposal, the European Data Protection Supervisor expresses the view that 'the intrusive character of the measures is evident. On the other hand, their utility is far from being demonstrated'. [38] On 28 October 2008, the European Union's Fundamental Rights Agency (FRA) also published an Opinion on the Proposal which critically looks at a number of the Proposal's provisions, including the open-ended and imprecise formulations, the necessity and proportionality of the measures envisaged, and the risk of discriminatory profiling.[39] According to the FRA, the European standard of data protection cannot always be ensured when personal data are processed outside the EU, therefore 'the transfer of PNR data to third countries creates the risk of serious infringements of fundamental rights'.

5.6 "Profiling"

Profiles are increasingly created, not by any one national police force (and/or secret service), but as part of international co-operation.

A number of 'elements' for these terrorist profiles, including nationality, travel document, method and means of travel, age, sex, physical distinguishing features (e.g. battle scars), education, choice of cover identity, use of techniques to prevent discovery or counter questioning, places of stay, methods of communication, place of birth, psycho-sociological features, family situation, expertise in advanced technologies, skills at using non-conventional weapons (CBRN), attendance at training courses in paramilitary, flying and other specialist techniques. According to one NGO, Privacy International, law enforcement agencies could then search through national databases hoping to identify equivalent elements in order to then presumably pinpoint terrorists.[40]

Such "intelligence-led profiling" is often presented by the authorities as somehow more acceptable, "softer", than crude discriminatory (racial/ethnic) profiling. In reality, there may be little difference: Targeting people because they fit a particular basic stereotype - being a young, practising Muslim, and having at some time travelled to Pakistan, for instance - *is* ethnic-racial-religious "profiling".[41]

The Fundamental Rights Agency in their Opinion on the Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes (28 October 2008) comment critically on the use of profiling within the the context of PNR data.

6. Assessment

States have a positive obligation to protect the lives of their citizens (*Osman v United Kingdom*).[42] They are obliged to do all that could be reasonably expected of them to avoid a real and immediate risk to life of which they have or ought to have knowledge. In this sense, the right to security has long been "codified" as a human right in the European Court of Human Rights (ECHR) case-law. This doctrine is equally applicable to life-threatening situations as a result of a terrorist threat. The preamble to the Guidelines on human rights and the fight against terrorism which the Council of Europe's Committee of Ministers adopted on 11 July 2002 refers to "the imperative duty of the States to protect their populations against possible terrorist acts".[43] The same consideration can be found in the Guidelines on the Protection of Victims of Terrorist Acts, adopted by the Committee of Ministers on 2 March 2005.[44]

However, in *Osman* the Court also stressed "*the need to ensure that the police exercise their powers to control and prevent crime in a manner which fully respects the due process and other guarantees which legitimately place restraints on the scope of their action to investigate crime and bring offenders to justice, including the guarantees contained in Articles 5 and 8 of the Convention*." States thus have the difficult job of balancing competing human rights interests. On the one hand, they must protect their population against terrorist threats, and on the other, they must safeguard the fundamental rights of individuals, including persons suspected or convicted of terrorist activities.

New technologies pose new threats to the individual in the "information society". There is greatly increased direct surveillance, through CCTV, car licence plate recognition systems, etc. There is a massive expansion in "dataveillance": the monitoring of the "data trails" left by individuals in numerous transactions, as described in this paper. And decisions on whom to "target" are increasingly taken by computers on the basis of effectively unchallengeable computer-generated "profiles".

There is another general trend to use administrative law, and administrative sanctions, to deal with "trouble-makers", in ways that by-pass the criminal law and that are thus not subject to the safeguards of the criminal justice system, or that modify the law (e.g. standards of proof and rules on the admissibility of evidence) in ways that seriously affect the rights of individuals.

Anti-terrorist and related policies give a clear impetus to these pre-existing trends: many measures are introduced, and accepted, as needed in the fight against "organised crime" and "terrorism" (with both being ill-defined). They are often too easily adopted on a supposedly temporary, "emergency" basis - but then, once introduced, become permanent and are extended into the general law. It is difficult to introduce sunset clauses into such legislation.

In the anti-terrorist context, the technologies involved may also lead to intrusive and punitive action - including administrative action - against large numbers of innocent civilians, without being effective in stopping real terrorists. What is more, computerised "profiling" risks discriminating against minority groups. Profiling can have a devastating effect on the individual, who is likely to be spied upon, harassed, refused permission to travel, denied a job or a research post, or even arrested. It will also have a chilling effect on democracy itself.

Moreover, any measure in which the concept of availability is used ought to be proportionate respecting the fundamental rights of the individual.

The targeting of "possible" criminals or terrorists, profiling, and abandoning purpose-limitation all result in the throwing together of all kinds of data, from all kinds of public and private-sector sources, "hard" and "soft", relating to suspects, witnesses, "contacts" and even victims. Such policies make the evaluation of this amalgamation of data impossible to assess or verify. Moreover (and as an inevitable consequence), they may deny those (seriously) affected by them any effective remedies.

7. Conclusions

We are rapidly becoming a "Surveillance Society". This is partly the result of general technical and societal developments, but these trends are strongly reinforced by measures taken in the fight against terrorism.

In the context of the fight against terrorism, this means individuals are at risk of being targeted for being suspected "extremists" or for being suspected of being "opposed to our constitutional legal order", even if they have not (yet) committed any criminal (let alone terrorist) offence.

"Targets" of this kind are moreover increasingly selected through computer "profiles". Even if some may be caught, there will always be relatively large numbers of "false negatives" - real terrorists who are not identified as such, and unacceptably high numbers of "false positives": large numbers of innocent people who are subjected to surveillance, harassment, discrimination, arrest - or worse. Freedom is being given up without gaining security.

In addition, increasing use is made of non-criminal, yet effectively punitive, "administrative" measures against identified suspected "extremists" or new-type "enemies of the State". This robs them of fundamental safeguards, both against the specific measures taken against them and, as groups, against such discrimination. It leads to alienation of the groups in question, and thus actually undermines security.

In the process, all of us are increasingly placed under general, mass surveillance, with data being captured on all our activities, on-line or in the "real" world. Such general surveillance raises serious democratic problems which are not answered by the repeated assertion that "*those who have nothing to hide have nothing to fear*."

The response to these developments should be a re-assertion of the basic principles of the Rule of Law, as enshrined, in particular, in the European Convention on Human Rights, and as further elaborated in the case-law of the European Court of Human Rights and the European Court of Justice, as well as in European legal instruments directly or indirectly inspired by the Convention and such case-law, including in particular the still-pre-eminent Council of Europe recommendation on data protection in the police sector (Recommendation R(87)15 of the Committee of Ministers).

The basic principles are well-established, and indicate the way forward:

I. Under the European Convention on Human Rights, the interferences with fundamental rights inherent in the measures described in this paper must be justified by the state as being:

- in accordance with the law;
- 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 crime or disorder; or
  - for the protection of the right and freedom of others;
- proportionate; and
- non-discriminatory.

II. The applicable data protection principles are equally well-developed, in Council of Europe Convention No. 108, Committee of Ministers Recommendation R(87)15, the main EC directive on data protection (Directive 95/46/EC), and in the case-law of the ECHR and the ECJ. They require *inter alia* that:

- All processing of personal data for law enforcement and anti-terrorist purposes must be based on clear and specific, binding, published legal rules.
- The collection of data on persons not suspected of involvement in a specific crime or of posing a threat, the collection of information through intrusive, secret means and the use of "profiling" techniques must be subject to a particularly strict "necessity" and "proportionality" test.
- Factual and intelligence data, and data on different categories of data subjects should be clearly distinguished.
- Access to police and secret service files should only be allowed on a case-by-case basis, for specified purposes and be under judicial control in the Member States.
- There must be limits on the storing of old information and on the time for which new information can be retained.
- The collection of data on individuals solely on the basis that they have a particular racial origin, particular religious convictions, sexual behaviour or political opinions or belong to particular movements or organisations which are not proscribed by law should be prohibited.

· Reliance by private or public bodies on computers to take decisions on individuals, without human input is fundamentally contrary to the requirement of respect for the human identity and should only be allowed exceptionally under strict safeguards.

- There must be strong safeguards established by law which ensure appropriate and effective supervision over the activities of the police and the secret services - also in the fight against terrorism. This supervision should be carried out by the judiciary and through parliamentary scrutiny. All personal data processing operations should be subject to close and effective supervision by independent and impartial data protection authorities.

III. In the fight against terrorism and organised crime, these principles should not be abandoned but, rather, re-asserted. Anti-terrorist "profiling" and EU cooperation on the basis of the "availability" principle as currently construed risk breaching these established standards. These policies and proposals should be reviewed to ensure that they comply with accepted European law, including the European Convention on Human Rights (as applied by the Strasbourg Court), CoE Convention 108 and CoE Recommendation R(87)15, and EC Directive 95/46/EC.

[1] Memorandum of Understanding between the Council of Europe and the European Union, adopted at the 117th Session of the Committee of Ministers, Strasbourg, 10-11 May 2007, COE Document M(2007)74 of 10 May 2007, para. 26 (in the section on Rule of law, legal co-operation and addressing new challenges).

[2] *Idem*, para. 47 (in the section on Inter-institutional co-operation).

[3] Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Program Assessment, study by the United States' National Research Council, 2008, Executive Summary, pp. 3-4. Or as it is put in somewhat greater detail in the body of the study: "*Automated terrorist identification is not technically feasible because the notion of an anomalous pattern - in the absence fo some well-defined ideas of what might constitute a threatening pattern - is likely to be associated with many more benign activities than terrorist activities. In this situation, the number of false leads is likely to exhaust any reasonable limit on investigative or analytical resources. For these reasons, the desirability of technology development efforts aimed at automated terrorist identification is highly questionable*." (pp. 78-79). For the full assessment, with extensive detail, see Appendix H: *Data Mining and Information Fusion*. The study is available at: http://www.nap.edu/catalog.php?record_id=12452.

[4] See, e.g., "*New study highlights discrimination in use of anti-terror laws*", press release on a study by the UK Institute for Race Relations (a Government body), published on 2 September 2004. The press release can be found at: http://www.irr.org.uk/2004/september/ak000004.html; the full study can be downloaded from: http://www.irr.org.uk/pdf/terror_arrests_study.pdf.

[5] See John Vervaele, *Terrorism and information sharing between the intelligence and law enforcement communities in the US and the Netherlands: emergency criminal law?* in: Utrecht Law Review, Volume 1, Issue 1 (September 2005), http://www.utrechtlawreview.org/.

[6] ECHR, 4 November 1950, ETS No. 5. Article 8(1) - Right to respect for private and family life **-** everyone has the right to respect for his private and family life, his home and his correspondence.

[7] *Peck v. the UK*, Judgment

[8] *Copland v. the UK*, Judgment of 3 April 2007.

[9] EU Charter of Fundamental Rights, Article 7 - Respect for private and family life - Everyone has the right to respect for his or her private and family life, home and communications. EU Charter of Fundamental Rights, Article 8 - Protection of personal data - (1) Everyone has the right to the protection of personal data concerning him or her.

(2) Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

(3) Compliance with these rules shall be subject to control by an independent authority.

[10] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No. 108, of 28 January 1981; Additional protocol to Convention 108 regarding supervisory authorities and transborder data flows, ETS No. 181, of 8 November 2001. For the full texts of both Convention No. 108 and this Additional Protocol, see: http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Data_protection/. Note that amendments to Convention No. 108 have been drafted and adopted by the Committee of Ministers to allow the EC (note: not the EU!) to become a party to the Convention: the amendments can also be found on that webpage. However, they have not yet come into force, and the EC is not yet a party.

[11] OJ L 281, 23.11.1995, p. 31: http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm. The requirements of the directive are described in detail in Douwe Korff, Data Protection Law in Practice in the European Union, Brussels/New York, 2005.

[12] Directive 2002/58/EC replaced an earlier directive, Directive 97/66/EC of the European Parliament and the Council of 4 November 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector (often referred to as "the ISDN Directive"). Both are again available from: http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm.

[13] The amendments were carried out by means of Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJL 105 13.04.2006 p. 54, again also available from: http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm.

[14] http://www.coe.int/t/e/legal_affairs/legal_cooperation/combating_economic_crime/1_standard_settings/Rec_1987_15.pdf.

[15] *Österreichischer Rundfunk v. Austria*, Joined Cases C-465/00 (Rechnungshof v. ÖRF et al.), C-138/01 and C-139/01 (respectively, Christa Neukomm and Lauermann v. ÖRF) (references for preliminary rulings from the Austrian Verfassungsgerichtshof and Oberster Gerichtshof respectively), Opinion of Advocate-General Tizzano of 14 November 2002; Judgment of 20 May 2003,; *Lindqvist v. Sweden*, Case C-101/01 Bodil Lindqvist v Åklagarkammaren i Jönköping (Reference for a preliminary ruling from the Göta Hovrätt), Opinion of Advocate-General Tizzano of 19 September 2002; Judgment of 6 November 2003. These judgments too are summarised in Douwe Korff, *Paper No. 4: The Legal Framework*, in: Ian Brown & Douwe Korff, Privacy & Law Enforcement (note 6, above), pp. 34-44.

[16] In *Copland* (note 7, above), the Court ruled that a vague "enabling" [*vires*] provision in English law was not sufficient: although regarded as adequate by the English courts, it did not constitute "law" in the ECHR-sense.

[17] Note that the Court clearly regards the gathering and keeping of information for intelligence files as, as such, "surveillance measures". This is not qualified by reference to the means used: "surveillance" is not limited to secret, technical means; it can also be kept on individuals by collecting information openly, or from public sources, e.g. from lists signed by people opposing the War In Iraq, or newspaper cuttings, or open photography or videoing of demonstrations.

[18] Cf. the *Klass*- and *Kopp*-judgments of the EuCtHR, expressly referred to in this respect in the Court's *Rotaru*-judgment.

[19] i2010 eGovernment Action Plan, For this plan, see: http://europa.eu/scadplus/leg/en/lvb/l24226j.htm

[20] *Idem*,

[21] EDPS Newsletter of 9 July 2007. For details, see Europol COM (2006) 817, Dec. 2006, on replacing the Europol Convention and *acquis* with a new Decision giving it operational powers.

[22] Eurojust's sister organisation, the European Judicial Network, established in 2001, operates in the field of civil and commercial law. See: http://ec.europa.eu/civiljustice/.

[23] See (e.g.) the Eurojust Annual Report 2006, p. 6. Available from: http://eurojust.europa.eu/press_releases/annual_reports/2006/Annual_Report_2006_EN.pdf.

[24] The letter can be found at: http://www.commissie-meijers.nl/assets/commissiemeijers/Commentaren/2007/CM0712-IV%20Comments%20Standing%20Committee%20on%20the%20use%20of%20Eurodac_EC.pdf.

[25] http://europa.eu/scadplus/leg/en/lvb/l33020.htm, under the heading "*The second-generation Schengen Information System (SIS II)*" It is also explained there that: "*Pending SIS II becoming operational, the Justice and Home Affairs Council of December 2006 gave its endorsement to the SISone4all project (a project of the Member States coordinated by Portugal). SISone4all is a temporary solution designed to connect nine EU-2004 member countries to the existing version of SIS1+ (with some technical adjustments) in order to allow these countries to complete the Schengen evaluations as soon as possible with a view to abolishing internal border controls. Work on SISone4all should be completed by the end of August 2007*." (SIS1+ is an already-improved version of the original SIS).

[26] House of Lords European Union Committee, Ninth Report, into the Schengen Information System, 20 February 2007, at: http://www.publications.parliament.uk/pa/ld200607/ldselect/ldeucom/49/4902.htm.

[27] *Idem*.

[28] EDPS Newsletter of 9 July 2007.

[29] Council Decision 2008/633/JHA of 23 June 2008

[30] Council Decision 2008/615/JHA of 23 June 2008 and 2008/616/JHA of the same date.

[31] Hague Programme on strengthening freedom, security and justice in the European Union, adopted by the European Council on 4 November 2004. See also the 2005 Council and Commission Action Plan implementing the Hague Programme on strengthening freedom, security and justice in the European Union. The definition provided here is quoted at: http://www2.poptel.org.uk/statewatch/news/2006/dec/p-of-a-art.pdf.

[32] http://www.cnpd.pt/bin/relacoes/declaration.pdf

[33] Under Council Directive 2004/82/EC.

[34] Proposal COM(2007)654 final.

[35] Agreement between the European Union and the United States of Amercia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS) (2007 PNR Agreement) OJL 204, 4.8.2007, p. 18).

[36] Agreement between the European Community and the Government of Canada on the processing of Advance Passenger Information and Passenger Name Record Data (OJ L 82, 21.3.2006, p.15). In respect of Australia (OJ 8.8.08)

[37] Joint opinion on the proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes, presented by the Commission on 6 November 2007, adopted by the Article 29 Working Party on 5 December 2007 and by the Working Party on Police and Justice on 18 December 2007, WP 145, WPPJ 01/07.

[38] http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2007/07-12-20_EU_PNR_EN.pdf

[39] http://fra.europa.eu/fra/material/pub/discussion/FRA_opinion_PNR_en.pdf

[40] Privacy International report on Discrimination and Anti-Terror Policy Across Europe, 20 September 2005, available from: http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-360509 (scroll down to section 2.2, "*Subtle Interventions and Surveillance*")

[41] See also General Policy Recommendation No. 11, Combating racism and racial discrimination in policing, European Commission against Racism and Intolerance (ECRI), 4 October 2007, CRI(2007)39.

[42] Judgment of 28 October 1998.

[43] Guidelines on human rights and the fight against terrorism, adopted by the Committee of Ministers on 11 July 2002 at the 804th meeting of the Ministers' Deputies.

[44] Guidelines on the Protection of Victims of Terrorist Acts, adopted by the Committee of Ministers on 2 March 2005 at the 917th meeting of the Ministers' Deputies
See also: Thomas Hammarberg, "Give victims of terrorism sustained compensation and support", speech at the 27th Conference of the European Ministers of Justice, "Victims: place, rights and assistance", Yerevan, Armenia, 12-13 October 2006, CommDH/Speech(2006)19.

Top