Project on Cybercrime
www.coe.int/cybercrime

Economic Crime Division
Directorate General of
Human Rights and Legal Affairs
Strasbourg, France

Version 25 March 2008

Cybercrime investigation and the protection of personal data and privacy

Discussion paper
prepared by
Rob van den Hoven van Genderen

This report has been prepared within the framework of the Project on Cybercrime of the Council of Europe.

Contact

For further information please contact:

Economic Crime Division
Directorate General of Human Rights and Legal Affairs
Council of Europe
Strasbourg, France

Tel: +33-3-9021-4506
Fax: +33-3-9021-5650
Email: alexander.seger@coe.int

Contents

1 Introduction

> The "propiska" is a device used all over Eastern Europe as a residence permit, tying each person, native-born or immigrant, to a single address. Propiski were introduced by the Tsar; Lenin banned them; Stalin reintroduced them; and the Constitutional Court banned them again in 1991. To no effect in Moscow, at least, where the Mayor announced that he intended to ignore the ban.[1]

The globalisation of economic, political and social activities, supported by an increasing use of the Internet and other information and communication technologies, raises a wide range of questions regarding privacy and the protection of personal data. This includes questions related to data protection principles, such as those established by the European Union and the Council of Europe (e.g. ETS 108 and Rec R(87)15 on the use of personal data in the police sector), and the investigation of cybercrime[2], but also questions related to data retention, the increasing trend towards authentication of ICT users, the relationship between service providers and law enforcement and others. Countries developing cybercrime legislation therefore need to be familiar with relevant privacy and data protection issues.

We see an increasing adaptation of "conventional" crime to cybercrime because of the digitalisation, convergence of technologies and globalisation of ICT. Traditional measures on investigations do not meet the demands of these changes, therefore special procedures need to be developed.

The question is, what measures can be taken by governmental and police authorities to adapt to and restrain this development in a way that existing privacy rights are preserved? To what extent are authorities free to use personal data and from what sources? There is publicly available data from the Internet and other public sources, but also data acquired in the execution of public tasks, often available in governmental databases. Are criminal investigators allowed to use the data in the same way other governmental authorities use these sources?

Because of the international nature of crimes, international co-ordinated investigations and the use of personal data must be made possible, but with a sharp eye on their limitations in the interest of human rights and specifically the protection of the privacy of individuals and taking into account the evolution of data availability.

The key questions to confront are: how can the tension between privacy protection and criminal investigation be regulated at acceptable levels? And; what adaptations to the existing regulatory framework are needed? In a study by Privacy International[3] many European states are not considered capable of upholding human rights standards on privacy. Only Greece is considered to have significant protection and safeguards. Maybe the present study can improve our "score".

---

1. A submission prepared exclusively for the Home Affairs Committee in connection with its inquiry into a Surveillance Society by David Moss of Business Consultancy Services Ltd., April 2007, http://dematerialisedid.com/BCSL/HAC3.pdf

2 See the procedural provisions of the Convention on Cybercrime.

3. 'Leading surveillance societies in the EU and the World 2007', 28/12/2007, www.privacyinternational.org/article.shtml?cmd[347]=x-347-559597

The purpose of this study is be to give insight and guidance to countries as to how to make cybercrime investigations compatible with data protection and privacy concerns, in particular when implementing the procedural provisions of the Convention on Cybercrime.

Certainly when an investigation into transborder dataflow is required, it is essential to have sufficient guarantees that authorities are not bypassing fundamental rights.

In the comments to the European Convention on Human Rights, it is recognised that essentially, it should make no difference for data users or data subjects whether data processing operations take place in one or in several countries. The same fundamental rules should apply and data subjects should be given the same safeguards for the protection of their rights and interests.

Although these rules apply, we must also ensure that they will not be bypassed in practice by investigative authorities and that deviations will only be possible in exceptional cases. In general this is an accepted principle of national and international laws, but in practice guarantees and policies in this respect are not very visible. European legal authorities should bear this in mind when exercising their authorities.

2 Cybercrime investigations and general privacy issues

2.1 The essence of personal data protection

Quote from a letter from the Netherlands Minister of the Interior and Kingdom relations:

> Above all the effort will be directed on the earliest identification of preparation of possible terroristic actions and its offenders. New forms of automated data-analysis will be used like the search on profiles and the recognition of patterns of behaviour by data-mining. Therefore large databases with personal data of non-suspects must be searched.[4]

Data protection is one of the essential fundamental rights and has to be preserved in a digital world as in the former analogue society. There must be an open eye for threats to society, internal and external, but fundamental rights such as privacy must be considered of great value for a democratic society and must be available for all persons on an equal basis.

In the evolution towards a digital society, many developments have taken place, but in essence it seems that not much has changed concerning the threats towards privacy in general and the validity of the fundamental essence of this right:

> Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right "to be let alone". Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops". For years there has been a feeling that the law must afford some remedy for the unauthorized circulation of portraits of private persons; and the evil of invasion of privacy by the newspapers.[5]

Next to the fact that Warren and Brandeis saw the threats to privacy developing out of modern society of more than 100 years ago, they also stated that privacy was a dynamic concept that can be adapted to the needs and values of individuals.

For a better understanding of the concept of privacy in relation to this study, I refer to the classification of Clarcke[6] in the following dimensions:

- **privacy of the person**, sometimes referred to as 'bodily privacy'. This is concerned with the integrity of the individual's body. Issues include compulsory immunisation, blood transfusion without consent, compulsory provision of samples of body fluids and body tissue, and compulsory sterilisation;
- **privacy of personal behaviour**. This relates to all aspects of behaviour, but especially to sensitive matters, such as sexual preferences and habits, political activities and religious practices, both in private and in public places. It includes what is sometimes referred to as 'media privacy';

4. Parliamentary White Papers (Kamerstukken II, 2003/04, 29 200 VII, nr 61, translated citation in Ruben Sietsma, p.13, Dataprocessing and datamining for investigating purposes. Considering the right on privacy (Gegevensverwerking in het kader van opsporing, toepassing van datamining ten behoeve van de opsporingstaak: afweging tussen het opsporingsbelang en het recht op privacy), Iter, Den Haag, 2006.
5. Warren and Brandeis, 'The Right to Privacy', *Harvard Law Review*, Vol. IV, Dec 15, 1890, No. 5.
6. Paper by Roger Clarcke, National University of Australia, www.anu.edu.au/people/Roger.Clarke/DV/Privacy.html

- **privacy of personal communications**. Individuals claim an interest in being able to communicate among themselves, using various media, without routine monitoring of their communications by other persons or organisations. This includes what is sometimes referred to as 'interception privacy'; and
- **privacy of personal data**. Individuals claim that data about themselves should not be automatically available to other individuals and organisations, and that, even where data is possessed by another party, the individual must be able to exercise a substantial degree of control over that data and its use. This is sometimes referred to as 'data privacy' and 'information privacy'.

Clarcke stated that with the close coupling that has occurred between computing and communications, particularly since the 1980s, the last two aspects have become closely linked. This is the primary focus of public attention and of this document. It is useful to use the term "information or informational privacy" to refer to the combination of communications privacy and data privacy.

How broad the sources of personal data can be considered is presented in the Dutch study of the Telematics Institute at the University of Twente and the University of Tilburg, in the light of converging technologies:

> Converging technologies enable an enormous increase in data collection and processing, which is occurring already as we write. Not only are data stored in ever more databases (e.g., Google, customer databases, social networking, e-community sites, loyalty schemes, CCTV images), but also, new types of data have appeared, such as location data (mobile phones), Internet surfing data, identification data (RFID), and DNA data (like geographic ancestry), that traditionally were not generated or processed. Moreover, it has also become much easier to process and use data, through digitisation, automated recognition, data sharing, and profiling. Increasingly, data collection can also take place unobserved (aerial photography, miniature cameras, directional microphones, micro sensors, 'smart dust'), using more senses than sight and sound (olfactory sensors, chemical 'cameras'). Much of this is not new, but the scale of data increase and the combination of all developments lead to a truly qualitative increase in the data 'out there' about citizens and their personal lives. [7]

With reference to the sensitive aspect in surveillance by authorities, it is also important to concentrate on sensitive personal data, as mentioned under the third point, and the use of body material for DNA research, as mentioned under the first point, be it that this all must be understood as personal data.

The concept of Alan Westin[8] still relates strongly to this conception of privacy: privacy is the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others. Viewed in terms of the relation of the individual to social participation, privacy is the voluntary and temporary withdrawal of a person from the general society through physical or psychological means, either in a state of solitude or small-group intimacy or, when in larger groups, in a condition of anonymity or reserve.

7. 'Security Applications for Converging Technologies Impact on the constitutional state and the legal order', Telematica Instituut, Enschede, Report TI/RS/2007/039, p. 109.
8. A.F. Westin, *Privacy and freedom*, 1967, New York 1967, p. 7.

2.2 Self-determination = self-limitation of privacy?

The question in relation to this study is of course whether privacy can give way to the interests of society, and more specifically to the interests of criminal investigations of the national and international law enforcement authorities,.

It is the choice of society as a collection of individuals to refer to a (natural) person and how these data are used for the good of the (sum) of these individuals.
This will account for the economic functioning of individuals in society as well non economic structures of the functioning of society.
It is the individual who has the control over these elements or data to decide how and to what extent these data are used[9]. How the individual can exercise this right should be based on the fact that privacy is actually a value, there must also be a (legal)mechanism to do that.

The above mentioned concept indicates that the fundamental value of this concept of privacy is the right to decide for oneself how to divulge the different elements of the so-considered privacy right as a set of rights connected to the information sphere of each individual. The question is how far the right of informational self-determination can be restricted in the so-called general interest. See in this respect the concept of "informational self-determination" in the 1983 decision of the German Federal Constitutional Court that stated a rather fundamental recognition of this right. This does not necessarily, of course, reflect the observation of other European countries

> Under the possibilities of modern data processing the protection of the individual against the unlimited storing, processing and transmission of his personal data of the fundamental personal right under Article 2.1 of the National Constitution. Art. 1.1 National Constitution will be guaranteed in so far that the individual himself will have the constitutional right to decide on the use and accessibility of his personal data.
> 2 Limitation of this right on „informational self-determination is only possible in the (general) national interest but must reflect the constitutional demand that this must be proportional and sanctioned by law10.

In the Netherlands, concerning the so-called "toll-driving" (*rekening rijden*) where the vehicle will be registered to pay for the use of Dutch highways, the discussion came up whether individuals had the right to "sell" their personal information to diminish the costs of the so-called "toll driving". This suggestion was also supported by the advice of the Dutch

[9] See also the discussion on "personhood" and digital identity in: Mary Rundle a.o., At a crossroads: "personhood" and digital identity in the information society, DSTI/DOC(2007)7

10.(original text in German) German Constitutional Court decision on a nation-wide "census" BVerfGE 65, 1 - VolkszählungUrteil des Ersten Senats vom 15. Dezember 1983. Unter den Bedingungen der modernen Datenverarbeitung wird der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG umfaßt. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.

2. Einschränkungen dieses Rechts auf "informationelle Selbstbestimmung" sind nur im überwiegenden Allgemeininteresse zulässig. Sie bedürfen einer verfassungsgemäßen gesetzlichen Grundlage, die dem rechtsstaatlichen Gebot der Normenklarheit entsprechen muß. Bei seinen Regelungen hat der Gesetzgeber ferner den Grundsatz der Verhältnismäßigkeit zu beachten. Auch hat er organisatorische und verfahrensrechtliche Vorkehrungen zu treffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken

Data Protection Authority. Only the strictly necessary data should be available to the government. Other "side-catch" information about itinerary, distance, speed and other information could be made available by the individual on his own merits
Of course the influence of the data subject on the processing of his personal information by authorities in criminal matters can not (always) be compared with day-to-day operations.
The question is whether "cybercrime" is so special that it requires that fundamental rights are bypassed more than for "ordinary" crime. I believe it is important to look at the effect of certain acts of criminal behaviour on (international) society as such and thus decide what instruments are needed.

Although some (international) crime needs more investigative powers and surveillance than other criminal activities, it is still necessary to guarantee the protection of fundamental privacy principles in national and international law. An automatic reaction to state that more investigative powers are needed to confront computer crime and terrorist actions is not per se the right answer. Proportionality and accountability in the use of these instruments should be held high in this respect.

2.3 Data protection in the global digital dimension

> Measures to prevent and punish terrorism must be conducted with respect for human rights. Nonetheless, when counter-terrorism methods shift from law enforcement to transnational armed conflict, the applicability and effect of particular positive human rights norms may change. If European states find it necessary to pursue the military model of counter-terrorism, then European human rights jurisprudence may need to modify its rigid opposition to military trials. The right to take proceedings before a court for determination of the lawfulness of detention provides an important procedural safeguard against torture and disappearance, but in some narrow circumstances derogation from that right may be strictly required by the exigencies of combating terrorism.[11]

In the equilibrium between security and privacy, the weight seems to be shifting towards security protection by giving up on human rights, including the protection of privacy. In the international treaties on human rights, data protection and/or the protection of privacy and/or personal life are widely considered to be building stones of a civilized society, although in 90% of the world the recognition of this principle is no guarantee that it is actually followed in national practice.

Of course, the principles of human rights treaties are not specifically intended for digital transfer of data on a global scale, but should be applicable on the protection of the principle as such in the use and processing of personal information, indiscriminately of the means of storage, transport or infrastructural aspects of the personal information.

As basic principles for the protection of privacy there are, besides other less fundamental treaties or conventions, three treaties relevant for this study that are widely recognised as the basis for the protection of privacy and personal life: Article 12 of the Universal Declaration of Human Rights of 1948, Article 17 of the International Covenant on Civil and Political Rights (ICCPR), and Article 8 of the European Convention for the Protection of

11. Neuman, Gerald, 'Comment, Counter-terrorist Operations and the Rule of Law', *The European Journal of International Law*, Vol. 15, No.5.

Human Rights and Fundamental Freedoms (ECHR). Also of importance are the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.[12]

The provisions dealing expressly with privacy are set out in Article 12 of the Universal Declaration of Human Rights, which states:

> No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

In almost identical terms, Article 17 of the ICCPR provides*:*

> 1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks upon his honour and reputation.
> 2. Everyone has the right to the protection of the law against such interference or attacks.

Whereas the above provisions are framed essentially in terms of a prohibition of "interference with privacy", the equivalent provisions of Article 8 of the ECHR are framed in terms of a right to "respect for private life":

> 1. Everyone has the right to respect for his private and family life, his home and 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 question can be posed: is there a difference between data protection and the protection of privacy and personal life? Bennet cites in his book *Regulating Privacy Justice*[13] that, in the concept of privacy, the spirit of individualism is not different from the start of privacy thinking in the 19th century, concerning thoughts, beliefs and feelings: "We want to decide for ourselves with whom and to what extent we are willing to share them." Further, he cites from a sociological point of view of Edward Shills, who stated that one's actions and their history belonged to the self which generated them and were to be shared only with those with whom one wished to share them.

2.3.1 Basic principles

As indicated above, the basic principles of data protection laws should encompass the following principles that can be derived from these international instruments which relate to the processing (i.e., collection, registration, storage, use and/or dissemination) of personal data.[14]

12. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1980.
13. C. J. Bennet, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*, Cornell University Press, 1992, p. 24, note 22.
14. There are four relevant instruments in this respect: (i) the CoE Convention on data protection (see *supra* No. 1); (ii) the EC Directive on data protection (see *supra* No. 2); (iii) the OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (Paris: OECD, 1980), adopted 23.9.1980; and (iv) the UN Guidelines Concerning Computerized Personal Data Files (Doc E/CN.4/1990/72, 20.2.1990), adopted by the UN General Assembly on 4.12.1990. Of these, only the first two listed are legally binding instruments. Note, however, that the CoE Convention does not require a CoE member state to implement its provisions until it is ratified by the state. A range of international instruments have also been adopted dealing with data protection for specified sectors of activity, but only one of these

By "personal data" we mean data (or information) that relate to, and allow identification of, individual physical/natural persons (and sometimes groups or organisations). The principles are cited in different legal instruments in slightly varying forms that will be also cited in other paragraphs of this study, but can be summarised as follows:

- personal data should be gathered by fair and lawful means (hereinafter termed "fair collection principle");
- the amount of personal data gathered should be limited to what is necessary to achieve the purpose(s) of gathering the data (hereinafter termed "minimality principle");
- personal data should be gathered for specified and lawful purposes and not processed in ways that are incompatible with those purposes (hereinafter termed "purpose specification principle");
- use of personal data for purposes other than those specified should occur only with the consent of the data subject or with legal authority (hereinafter termed "use limitation principle");
- personal data should be accurate, complete and relevant in relation to the purposes for which they are processed (hereinafter termed "data quality principle");
- security measures should be implemented to protect personal data from unintended or unauthorised disclosure, destruction or modification (hereinafter termed "security principle");
- data subjects should be informed of, and given access to, data on them held by others, and be able to rectify these data if inaccurate or misleading (hereinafter termed "individual participation principle"); and
- parties responsible for processing data on other persons should be accountable for complying with the above principles (hereinafter termed "accountability principle").

The OECD Guidelines are based on comparable principles[15]:

Basic principles of national application

- Collection Limitation Principle

7. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

- Data Quality Principle

8. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

- Purpose Specification Principle

9. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

---

instruments is legally binding: this is the EC Directive 97/66/EC on the processing of personal data and the protection of privacy in the telecommunications sector (OJ No L 024, 30.1.1998, 1), adopted 15.12.1997.

Ibid, 151–152, and references cited therein; M Nowak, *U.N. Covenant on Civil and Political Rights: CCPR Commentary* (Kehl am Rhein/Strasbourg/Arlington: Engel, 1993), xix.

15. www.oecd.org/sti/security-privacy

- Use Limitation Principle

10. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9, except:
a) with the consent of the data subject
b) by the authority of law.

In the Council of Europe Convention for the Protection of Individuals, with regard to automatic processing of personal data (ETS 108) these principles are summarised in Article 5:

> **Quality of data**
>
> Personal data undergoing automatic processing shall be:
>
> a obtained and processed fairly and lawfully;
> b stored for specified and legitimate purposes and not used in a way incompatible with those purposes;
> c adequate, relevant and not excessive in relation to the purposes for which they are stored;
> d accurate and, where necessary, kept up to date;
> e preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.[16]

Although the police investigations relating to cybercrime may surpass certain aspects of privacy protection, these principles have to be taken into account when any measures are taken in investigations and processing personal data. At least it should be specified why those principles are not applicable in certain cases or circumstances.

2.3.2 Digital world

Although digitalisation should not affect the principle of protection of privacy and personal life as such, it is widely recognised that the use of digital data and the Internet will promote the use and interchange of data on a transborder level. See the explanatory report of the European Convention ETS 108:[17]

> Further growth of automatic data processing in the administrative field is expected in the coming years *inter alia* as a result of the lowering of data processing costs, the availability of "intelligent" data processing devices and the establishment of new telecommunication facilities for data transmission.

"Information power" brings with it a corresponding social responsibility of the data users in the private and public sector. In modern society, many decisions affecting individuals are based on information stored in computerised data files: payroll, social security records,

16. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108).
17. Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS 108). And the Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS 189), Strasbourg, 28.I.2003

medical files, etc. It is essential that those responsible for these files should make sure that the undeniable advantages they can obtain from automatic data processing do not at the same time lead to a weakening of the position of the persons on whom data are stored.

One could argue that digitalization is a cause or occasion to commit new forms of crime, which brings a need for more powerful authorities or measures in order to be able to gather evidence, including identification of the perpetrator. Access and use of personal data files are also used by the "criminal enemy" and therefore necessary to combat crimes. Another point of view is that "new" computer crimes exist of conventional crimes with other methods as for instance computer fraud but also the mentioned crimes in the additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems could be considered as existing criminal acts for which the means are present in existing criminal law, be it that investigations are getting more complicated.

As Dutch police described in their report combating crime is made even more difficult by IT developments, due to the increased methods of (electronic) communication, electronic surveillance and intelligence by criminal parties, vast digital files, globalisation and the volatility and insecurity of digital documents.

The recurring question is of course whether the IT orientation in society and increasing complexity in criminal investigations would give reason to set aside certain principles of "fair treatment" of personal data. I would argue that this is the ultimate reason to be even more prudent in using personal data. Question is, what do criminal authorities need to investigate and still act in conformity with privacy protection principles?

As a clear example we can refer to the way the UN treats digital personal data and apply these principles that are for the most also mentioned under paragraph2.3.1 in a way investigations still can be performed and the information can be processed:

United Nations guidelines concerning computerized personal data files[18]

How to deal with computerized files concerning personal data

The procedures for implementing regulations concerning computerized personal data files are left to the initiative of each State subject to the following orientations:

A. Principles concerning the minimum guarantees that should be provided in national legislations

1. Principle of lawfulness and fairness

2. Principle of accuracy

.

3. Principle of the purpose- specification

[18] adopted by the General Assembly on 14 December 1990

The purpose which a file is to serve and its utilization in terms of that purpose should be specified, legitimate and(…)

- All the personal data collected and recorded remain relevant and adequate to the purposes so specified;
- None of the said personal data is used or disclosed, except with the consent of the person concerned, for purposes incompatible with those specified;
- The period for which the personal data are kept does not exceed that which would enable the achievement of the purpose so specified.

4. Principle of interested-person access

5. Principle of non-discrimination

Subject to cases of exceptions restrictively envisaged under principle 6, data likely to give rise to unlawful or arbitrary discrimination, including information on racial or ethnic origin, colour, sex life, political opinions, religious, philosophical and other beliefs as well as membership of an association or trade union, should not be compiled.

Also here it is possible to make exemptions:

6. Power to make exceptions

Departures from principles 1 to 4 may be authorized only if they are necessary to protect national security, public order, public health or morality, as well as, inter alia, the rights and freedoms of others, especially persons being persecuted (humanitarian clause) provided that such departures are expressly specified in a law or equivalent regulation promulgated in accordance with the internal legal system which expressly states their limits and sets forth appropriate safeguards.

Exceptions to principle 5 relating to the prohibition of discrimination, in addition to being subject to the same safeguards as those prescribed for exceptions to principles 1 and 4, may be authorized only within the limits prescribed by the International Bill of Human Rights and the other relevant instruments in the field of protection of human rights and the prevention of discrimination.

7. Principle of security

Appropriate measures should be taken to protect the files against both natural dangers, such as accidental loss or destruction and human dangers, such as unauthorized access, fraudulent misuse of data or contamination by computer viruses.

8. Supervision and sanctions

The law of every country shall designate the authority which, in accordance with its domestic legal system, is to be responsible for supervising observance of the principles set forth above. This authority shall offer guarantees of impartiality, independence vis-à-vis persons or agencies responsible for processing and establishing data, and technical competence. In the event of violation of the provisions of the national law implementing the aforementioned principles, criminal or other penalties should be envisaged together with the appropriate individual remedies.

9. Transborder data flows

When the legislation of two or more countries concerned by a transborder data flow offers comparable safeguards for the protection of privacy, information should be able to circulate as freely as inside each of the territories concerned. If there are no reciprocal safeguards, limitations on such circulation may not be imposed unduly and only in so far as the protection of privacy demands.

10. Field of application

> The present principles should be made applicable, in the first instance, to all public and private computerized files as well as, by means of optional extension and subject to appropriate adjustments, to manual files. Special provision, also optional, might be made to extend all or part of the principles to files on legal persons particularly when they contain some information on individuals.

2.3.3 Handling of the information

In its General Comment 16, the Human Rights Committee of the UN has stated that Article 17 requires legal implementation of essential data protection guarantees in both the public and private sector. In the words of the Committee:

> The competent public authorities should only be able to call for such information relating to an individual's private life the knowledge of which is essential in the interests of society as understood under the Covenant. [...] The gathering and holding of personal information on computers, databanks and other devices, whether by public authorities or private individuals and bodies, must be regulated by law. Effective measures have to be taken by States to ensure that information concerning a person's private life does not reach the hands of persons who are not authorized by law to receive, process and use it, and is never used for purposes incompatible with the Covenant. In order to have the most effective protection of his private life, every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes. Every individual should also be able to ascertain which public authorities or private individuals or bodies control or may control their files. If such files contain incorrect personal data or have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination.

It would be a bit naive to assume that privacy right are fully respected in case of criminal investigations and the use of electronic (personal) data if only these principles are followed.

Although in principle 6 departure of the foregoing principles will be accepted, the departures have to be sanctioned by law. The problem is that the exceptions are defined too generally to be an acceptable control mechanism for an independent authority without more specified set limitations on the competences of investigative officials.

It is interesting to note that in the Islamic sphere, the Cairo Declaration on Human Rights in Islam of 5 August 1990 expressly recognises a right to privacy for all individuals without reservations:

> Article 18
>
> (a) Everyone shall have the right to live in security for himself, his religion, his dependents, his honour and his property.
>
> (b) Everyone shall have the right to privacy in the conduct of his private affairs, in his home, among his family, with regard to his property and his relationships. It is not permitted to spy on him, to place him under surveillance or to besmirch his good name. The State shall protect him from arbitrary interference.

(c) A private residence is inviolable in all cases. It will not be entered without permission from its inhabitants or in any unlawful manner, nor shall it be demolished or confiscated and its dwellers evicted.[19]

The fact that there are no reservations will not guarantee though that these rights will not be invaded. But it is interesting to note that Islamic countries do not see the necessity to make those reservations in this human rights declaration, contrary to the comparable international legal instruments of western societies. How the human rights, including the right on privacy are handled by the Islamic countries in practice though, will not be subject of this study.

2.4 Overview of the regulatory framework (EU, CoE)

2.4.1 The European Union

For the purpose of this study we may make a comparison with European legal instruments to protect personal data. But existing instruments at the European Union level do not suffice in respect. 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 does not apply to the processing of personal data in the course of an activity which falls outside the scope of Community law, such as those provided for by Title VI of the Treaty on European Union and on top of that will not apply to all countries of the Council of Europe.
As more specific applications additional to the aforementioned international general treaties on human rights, the Convention for the protection of individuals with regard to automatic processing of personal data is the standard reference document to analyse the extent of what is acceptable in policing by governmental authorities in relation to the cybercrime investigation.

2.4.2 Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data (ETS 108)

The convention's point of departure is that certain rights of the individual may have to be protected vis-à-vis the free flow of information regardless of frontiers, the latter principle being enshrined in international and European instruments on human rights (see Article 10, ECHR; Article 19, International Covenant on Civil and Political Rights). Where the present convention imposes certain restrictions or conditions on the exercise of freedom of information, it does so only to the extent strictly justified for the protection of other individual rights and freedoms, in particular the right to respect for individual privacy (see Article 8, ECHR). The convention consists of three main parts:

- substantive law provisions in the form of basic principles;
- special rules on transborder data flows;

19. Article 18 Cairo Declaration on Human Rights in Islam, (UN Doc A/45/421/5/21797, 199).
Citation note: also, for instance, that the jurisprudence of the European Court of Human Rights has generally exercised considerable influence on the decision making of the Inter-American Court of Human Rights, which is charged with hearing and determining complaints of breaches of the ACHR: see JG Merrills, *The Development of International Law by the European Court of Human Rights* (Manchester: Manchester University Press, 1993, 2nd ed), 18–19 and cases cited therein.

- mechanisms for mutual assistance and consultation between the Parties.

2.4.2.1 Private and public obligations

The Convention applies to the public as well as the private sector. Although most international data traffic occurs in the private sector, the convention is nevertheless of great importance for the public sector, and this for two reasons. First, Article 3 imposes obligations on the member states to apply data protection principles even when they process public files – as is usually the case – entirely within their national borders. Secondly, the convention offers assistance to data subjects who wish to exercise their right to be informed about their record kept by a public authority in a foreign country.

The distinction public sector/private sector is not found in the other provisions of the convention, especially since these terms may have a different meaning in different countries. However it may play a role in the declarations which the Parties may make with regard to the scope of the convention (paragraph 2).

> 34. *Paragraph 2.a.* It should be emphasised that exclusions from the scope of the convention are permitted only with respect to those categories of data files which are not or not yet subject to data protection legislation domestically.
> As for categories of data files which are subject to such legislation, derogations are permitted only under Article 9.
>
> 35. It is understood that any exceptions must be clearly specified. Otherwise, problems of interpretation would arise for other Contracting States to determine the scope of an exception, thus seriously hampering the application of the convention.

As stated above in par. 2.3.2 social responsibility concerning information power should be the point of departure, taken in mind when one considers developing the policy powers within the Cybercrime treaty. It cannot be accepted that the privacy position of individuals, certainly those who are not convicted at the end of criminal procedures will be put aside in a general way. There must be a clear separation in the different phases of collection of personal data and the use of powers in the investigative process and the actual criminal process if there is a clear causality between suspect and crime.

> It is essential that those responsible for these files should make sure that the undeniable advantages they can obtain from automatic data processing do not at the same time lead to a weakening of the position of the persons on whom data are stored.

.

Special attention should be given to the following provisions:

> **Article 6 – Special categories of data**
>
> Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions.

Article 8 – Additional safeguards for the data subject

Any person shall be enabled:

a to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file;

b to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form;
The provisions set out in this article are designed to enable a data subject to defend his rights vis-à-vis automated data files. Although in domestic legislation the contents of Article 8 clearly correspond to subjective rights, the present text expresses them in the form of safeguards which Contracting States offer to data subjects, in view of the non self-executing character of the convention. These safeguards include four main elements:

– knowledge about the existence of an automated data file;
– knowledge about the contents of the information, if any, stored about data subjects in a file;
– rectification of erroneous or inappropriate information;
– a remedy if any of the previous elements are not respected.

c to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of this convention;

d to have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to in paragraphs b and c of this article is not complied with.

Article 9 – Exceptions and restrictions

1 No exception to the provisions of Articles 5, 6 and 8 of this convention shall be allowed except within the limits defined in this article.

2 Derogation from the provisions of Articles 5, 6 and 8 of this convention shall be allowed when such derogation is provided for by the law of the Party and constitutes a necessary measure in a democratic society in the interests of:

a protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences;

b protecting the data subject or the rights and freedoms of others.

3 Restrictions on the exercise of the rights specified in Article 8, paragraphs b, c and d, may be provided by law with respect to automated personal data files used for statistics or for scientific research purposes when there is obviously no risk of an infringement of the privacy of the data subjects.

In the comments to the Convention it is stated that exceptions to the basic principles for data protection are limited to those which are necessary for the protection of fundamental values in a democratic society. The text of the second paragraph of this article has been modelled after that of the second paragraphs of Articles 6, 8, 10 and 11 of the European

Human Rights Convention. It is clear from the decisions of the Commission and the Court of Human Rights relating to the concept of "necessary measures" that the criteria for this concept cannot be laid down for all countries and all times, but should be considered in the light of the given situation in each country.

The question is whether an exception for "computer crime" is applicable in this case being a special situation for all member states. That would depend on the impact of the (security) effects on society as such. But this would not automatically give judicial or police authorities the right not to adhere to the agreed principles of fair treatment of personal data and not fulfilling all duties of authorities that come with it. This principle should certainly apply in the case of "pre-investigative" data collection[20].

2.5 Defining data protection as an evolutionary concept in the Convention for the Protection of Individuals with regard to automatic Processing of Personal Data (ETS 108)

It must be clear that the object of this Convention is to strengthen data protection, i.e. the legal protection of individuals with regard to automatic processing of personal information relating to them. There is a need for such legal rules in view of the increasing use made of computers for administrative purposes. Compared with manual files, automated files have a vastly superior storage capability and offer possibilities for a much wider variety of transactions, which they can perform at high speed.

Further growth of automatic data processing in the administrative field is expected in the coming years *inter alia* as a result of the lowering of data processing costs, the availability of "intelligent" data processing devices and the establishment of new telecommunication facilities for data transmission.

As stated in the introduction to the Convention for the protection of individuals with regard to automatic processing of personal data the possible use and possession of personal data by authorities gives the more reason to be extremely careful:

> For this reason, they should maintain the good quality of the information in their care, refrain from storing information which is not necessary for the given purpose, guard against unauthorized disclosure or misuse of the information, and protect the data, hardware and software against physical hazards.

As we can see, the development of techniques makes it increasingly possible to derive personal information from different sources. Nowadays it is possible to analyse body parts as small as a human hair to get personal information.

---

[20] Per analogiam: 56. Littera a *in paragraph 2* lists the major interests of the State which may require exceptions. These exceptions are very specific in order to avoid that, with regard to the general application of the convention, States would have an unduly wide leeway.
States retain, under Article 16, the possibility to refuse application of the convention in individual cases for important reasons, which include those enumerated in Article 9.
The notion of "State security" should be understood in the traditional sense of protecting national sovereignty against internal or external threats, including the protection of the international relations of the State

Therefore the notion that (identifiable)personal data (and its protection) is defined as far as it can practically derived from any source is considered to be extending in a continuous pace "personal data" means any information relating to an identified or identifiable individual ("data subject");

Although there used to be a distinction in treatment of directly or indirectly identifying data concerning the intrusion of privacy, the technological developments have made this distinction extinct[21] as stated also in the reference to the convergent technologies (note 6). For instance it is now widely recognized(WP29 and DPA) that IP-addresses are to be considered personal data.

2.6 Criteria for personal data protection and the existence of a right on informational self-determination

As stated in the introduction, it is important to see whether (under certain circumstances) it will be possible to let individuals decide if they make their personal information available to third parties, be it (inter-) national authorities or other third (commercial) parties.

Of course this is dependent on the purpose for which the information is intended to be used. In the example of personal information to diminish the costs of "toll driving", this suggestion was also supported by the advice of the Dutch DPA, where only the strictly necessary data should be available to the government or controller. In this case the data subject decides about the divulging of his personal information on his own merits.[22]

On the other hand, it cannot be that in cases of prosecution of crime the subject should have the right to decide what information he would make available; although it is widely accepted that a subject in a prosecution has the right not to incriminate himself (cautio) "you have the right to remain silent".[23] A comparable right is conceivable concerning (digital) information. "You have the right not to transfer to judicial parties any personal information that can incriminate yourself" - at least, not without a court order.

2.7 The double role of government as provider of personal data; what protective measures for government and data subjects?

Governments take the protection of privacy serious. On the basis of a Dutch proposal, the Council of Europe's Committee of Ministers adopted a declaration on human rights and the Internet[24] that was prepared by a special committee of academic experts and government representatives. According to the press release, "the declaration is the first international attempt to draw up a framework on the issue and breaks ground by up-dating the principles of the European Convention on Human Rights for the cyber-age".[25]

21. Dutch DPA Guidelines *Publication of personal data on the Internet*, December 2007. Page 10: The most well-known directly identifying item of data is the combination of forename and surname. The most well-known indirectly identifying items of data include (e-mail) addresses, telephone numbers, car number plates and the combination of post code/house number. Other indirectly identifying data include data regarding a person's characteristics, beliefs or behaviours that distinguish that person from others, for instance, the director of a specifically named company.
22. Ibidem note 7.
23. In the Netherlands CCP, Article 29.
24. CM(2005)56 final 13 May 2005, www.minbzk.nl/contents/pages/42826/declaration.pdf
25. www.edri.org/edrigram/number3.10/CoE

It strongly reaffirms that all rights enshrined in the Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) remain fully valid in the information age and should continue to be protected regardless of new technological developments, of course with all possible provisions that allow deviation from those principles. If need be, it is declared that:

> When circumstances lead to the adoption of measures to curtail the exercise of human rights in the Information Society, in the context of law enforcement or the fight against terrorism, such measures shall comply fully with international human rights standards. These measures must be lawful and defined as precisely as possible, be necessary and proportionate to the aim pursued, and be subject to supervision by an independent authority or judicial review.[26]

On the aspect of privacy it is stated that "any use of ICTs should respect the right to private life and private correspondence. The latter should not be subject to restrictions other than those provided for in Article 8 of the ECHR, simply because it is carried in digital form."[27]

The EDRI is of the opinion that although the declaration contains a very reassuring confirmation of the rights in the information age the declaration does not offer any specific new rights to Internet users when it comes to privacy. Several rights and freedoms are mentioned and reaffirmed repeatedly in the declaration; they are balanced against 'challenges' posed by the Internet, such as violation of intellectual property rights, access to illegal and harmful content and "circumstances that lead to the adoption of measures to curtail the exercise of human rights in the Information Society in the context of law enforcement or the fight against terrorism."

2.7.1 Which governmental agencies are allowed to exchange data

In the area of national and international criminal and security issues, police agencies and security organisations have to be defined. It is necessary to define the situation in which the exchange of personal data is deemed essential. In these cases a transparent procedure must be visible in the regulations.

In "supporting police tasks" it is allowed in the Netherlands to make databases and data as such available for (any) authorised personnel.[28] The purpose and the authorised persons who will use this information have to be described in writing.

Although in "police matters" there is a certain protection of privacy rights (see section 3.2), the control on intelligence agencies is almost not existent. The interchange between police and national and international intelligence agencies still takes place without any control mechanism. On the basis of, for example, the exception of Article 8 of the ECHR and mentioned comparable exceptions – "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"[29] – there is ample opportunity for the General Intelligence Agencies to obtain and exchange information.

26. Declaration of the Committee of Ministers on human rights and the rule of law in the Information Society, CM(2005)56 final, 13 May 2005.
27. ibid.
28. Article 13, Police Data Act.
29. Convention for the Protection of Human Rights and Fundamental Freedoms (ETS No. 005), Article 8.

In the Netherlands any person or governmental or non-governmental agency has to hand over any data to officials of the General Intelligence Service without real control.[30] But even this article was considered to be too restrictive. In a proposal to change the law, it was considered to explicitly mention communication service providers and the use of data analysis. There is no reference at all to any action to protect privacy or give any guarantee that use of personal information will be proportionate and purpose related.[31]
Although it must be stated that the exchange of information between police and the security agencies, at least in the Netherlands, is not a smooth process in it self. Because of bureaucratic and competence issues there are ample barriers to exchange of personal and other data concerning terroristic and other criminal activities[32]

2.7.2 Security issues

In several acts and regulations it is obligatory for governmental and non-governmental institutions to take all necessary (technical) measures to protect personal data, as stated in Article 7 of the European Data Protection Convention (ETS 108) of 1981. Certainly when personal information is transferred to different (international) services, the risk of vulnerability of the data is increased. This was also considered by the Dutch DPA concerning the Act on use of the personal identification service number (*burger service nummer*).[33]

The more data is transferred or processed in different places, the greater the risk that parties who are not intended to use this information will have access to it. In the Convention on Cybercrime itself, Articles 2 and 3 ask for measures against illegal access and interception. Obviously the judicial authorities have to take all technical and procedural measures to protect personal data files against any intrusion. If not, they could be held liable by the data subjects.

2.8 The role of government as user of personal data

It is clear that governmental institutions hold vast databases of personal information connected to easily identifiable characteristics, such as the personal identification service number (*burger service nummer*). This PIN is connected to tax issues, social security, etc.

The Dutch DPA severely criticised this Act on the Use of Personal Identification because it had no guarantees that the coupling of data would be in accordance with privacy requirements[34], although this danger was identified beforehand by parliament. The

30.Translation of Dutch Title: Act on Information and Security Services (Wet op de Inlichtingen en veiligheidsdiensten), 2002, Article 17 : The services are competent in the exercise of their task or in the support of their task to extract, collect or compile any data or information from any public authority, civil servant or any other person who is deemed to posess or can provide the necessary information (translation of Dutch:De diensten zijn bevoegd zich bij de uitvoering van hun taak, dan wel ter ondersteuning van een goede taakuitvoering, voor het verzamelen van gegevens te wenden tot:a. bestuursorganen, ambtenaren en voorts een ieder die geacht wordt de benodigde gegevens te kunnen verstrekken; b. de verantwoordelijke voor een gegevensverwerking).
31. See also advice of the DPA, 20 December 2007, www.cbpweb.nl
32 Report of the Supreme Audit Institution „nationale Rekenkamer“ of 10 april 2003 on the exchange of information concerning investigation and terrorism.
33. Advice of DP, 25 December 2005, Wet algemene bepalingen burgerservicenummer (30 312).
34. ibidem note 21;
In parliamentary whitepapers about this subject (a.o.TK 2002-2003, 28 600 VII,
nr. 6) stelde de regering onder meer het volgende: “Government will have to take the necessary measures, to take care that coupling of data and standing privacy rules will be in adjustment. On top of that it is the duty of the government to exercise a maximum in transparency and contolability . Neither of these intentions seems to be supported in the underlying draft bill by tangible measures. (*De overheid zal daarom de nodige maatregelen moeten treffen, om te beginnen door te zorgen, dat de koppeling van gegevens en*

government should certainly not automatically hold the competence to use all personal information if it concerns security or computer crime issues. It should be clearly stated in regulations when and under what circumstances personal data can be processed. It is of the utmost importance that there is no "easy exchange" between governmental agencies from, for instance, the Ministry of Finance to the Department of Justice, without guarantees given by law.

Recently a request for a proposal was made by the government to make inventories about what paragraphs exist in the different formal and material law to make an exchange of personal information possible.

2.8.1 Retention issues, the use of data available with other parties (Retention directive 2006)

> To investigate and prosecute crimes involving the use of the communications networks, including the Internet, law enforcement authorities frequently use traffic data when they are stored by service providers for billing purposes. As the price charged for a communication is becoming less and less dependent on distance and destination, and service providers move towards flat rate billing, there will no longer be any need to store traffic data for billing purposes. Law enforcement authorities fear that this will reduce potential material for criminal investigations and therefore advocate that service providers keep certain traffic data for at least a minimum period of time so that these data may be used for law enforcement purposes[35]

Taking into account the above, it took the European Commission five years to produce a directive based on the principle that traffic data should be available (at all times) to authorities for criminal investigations and other anti-terrorist actions, etc. In its Considerations, reference is made to the applicability of the privacy directive and the ePrivacy directive.[36]

> (3) Articles 5, 6 and 9 of Directive 2002/58/EC lay down the rules applicable to the processing by network and service providers of traffic and location data generated by using electronic communications services. Such data must be erased or made anonymous when no longer needed for the purpose of the transmission of a communication, except for the data necessary for billing or interconnection payments.
>
> (4) Article 15(1) of Directive 2002/58/EC sets out the conditions under which Member States may restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of that Directive. Any such restrictions must be necessary, appropriate and proportionate within a democratic society for specific public

---

de geldende privacywetgeving met elkaar in overeenstemming blijven. Daarnaast is het de plicht van de overheid om een maximale transparantie en controleerbaarheid te betrachten".
Geen van beide voornemens lijken in het voorliggende wetsvoorstel van concrete maatregelen te zijn voorzien).

35. EU Forum on Cybercrime Discussion Paper for Expert's Meeting on Retention of Traffic Data, 6 November 2001,

36. 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 (3) requires Member States to protect the rights and freedoms of natural persons with regard to the processing of personal data, and in particular their right to privacy, in order to ensure the free flow of personal data in the Community and. (2) 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 (Directive on privacy and electronic communications) (4) translates the principles set out in Directive 95/46/EC into specific rules for the electronic communications sector.

order purposes, i.e. to safeguard national security (i.e. State security), defence, public security or the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communications systems.

(8) The Declaration on Combating Terrorism adopted by the European Council on 25 March 2004 instructed the Council to examine measures for establishing rules on the retention of communications traffic data by service providers.

…

Because retention of data has proved to be such a necessary and effective investigative tool for law enforcement in several Member States, and in particular concerning serious matters such as organised crime and terrorism, it is necessary to ensure that retained data are made available to law enforcement authorities for a certain period, subject to the conditions provided for in this Directive. The adoption of an instrument on data retention that complies with the requirements of Article 8 of the ECHR is therefore a necessary measure.

The Retention directive is applicable on almost al communication data and all kind of communication services, without a clear distinction between public and private communication: (a) 'data' means traffic data and location data and the related data necessary to identify the subscriber or user;

There is a vast number of data aspects that are mentioned in Article 5 of the directive that have to be retained by the communication service providers. This obligation also applies to unsuccessful call attempts where those data are generated or processed, and stored (as concerns telephone data) or logged (as concerns Internet data), by providers of publicly available electronic communications services or of a public communications network.

The vast category of different sorts of data does not seem to be disputed, although it seems to be a too general and not very well defined area. All data concerned with communication traffic that can lead to any identification is to be retained and accessible for policing authorities. However the Dutch DPA seems to be only concerned with the period of retention. The Dutch DPA and the Article 29 Working Party have regularly asserted the position that the introduction of an obligation to retain historical traffic data of all citizens would be a very intrusive measure, whose need would have to be demonstrated irrefutably. In Article 8 of the European Convention on Human Rights (ECHR), the fundamental right of citizens is enshrined in of respect for their private life. The government may only infringe on that right to the extent that it is necessary in a democratic society. The necessity imposes high requirements on the proportionality of each specific measure that limits the private life of citizens. The general provisions from the Directive do not alter the fact that each national implementation must be tested independently against Article 8 of the ECHR and the corresponding ECHR case law. This applies specifically to the need for a retention period longer than the period necessary for the commercial purpose of provisioning electronic communication networks and services.[37]

The Dutch Minister of Justice stated, in answering the questions of Members of Parliament, that a retention period of 18 months was not disproportionate and can be necessary for complex investigations, legal help requests and cold cases. He was not capable to factually

37 www.cbpweb.nl

support his view on the question of how many cases could not be solved because of insufficient data in this perspective by reason.[38]

In Article 10 of the retention directive there is a (future) obligation to provide statistics of retention cases to the European Commission.

One could state that this directive is going beyond the meaning of article 20 CoC concerning the real time collection of traffic data. Competent authorities should be able to collect or record through the application of technical means on the territory of that party and compel a service provider, within its existing technical capability, to collect or record through the application of technical means on the territory of that party, or to co-operate and assist the competent authorities in the collection of recording of traffic data, in real time, associated with specified communications in its territory, transmitted by means of a computer system. The same applies to the interception of content data as is mentioned in Article 21. This is specified in Principle 2.1 of Recommendation R (87) 15 where the collection of personal data (that is, any information relating to an identified or identifiable individual) should be limited to such as is necessary for the prevention of a real danger or the suppression of a specific criminal offence. Any exception to this provision should be the subject of specific national legislation
Point is that articles 20 and 21 CoC give no limitation whatsoever on the use of this measure. Should this measures only be applied in a specific criminal offence, as it lays a burden upon the service provider and those of who the subject of this measure? Now it is left to the domestic legislator to provide for conditions and safeguards . The negative aspect of this freedom for legislators is that there will be no harmonized system of conditions and safeguards. Although one must recognize the fact that is hardly impossible to harmonize criminal procedures in this respect among the Member States

2.8.2 Rights of the data subject: information, notification and control

It is very important that Governments uphold the principles as set out in the first paragraph of this study, even within investigative work. In most national and international regulations, this principle is more or less well described in different articles in national data protection law based on Article 8 of the Convention, as stated under section 2.3.2, as already cited in the considerations of the Convention on Cybercrime.
In R (87) 15 principle 6 it is stressed that the supervisory authority should take measures to inform the public of the existence of files which are the subject of notification as well as of its rights in regard to these files. In addition, they should inform the public of possibilities to access a police file at reasonable intervals and without excessive delay, in accordance with the arrangements provided for by domestic law. We see that in Articles 18, 19 and 20, no reference is made to this possibility. The question is if reference to Articles 14 and 15 CoC gives enough guarantees. In practice it will scarcely happen that during the investigative process any data subject will be informed or that he will have any chance to have influence on the use of his personal data.

It would be advisable though, to agree on procedures how to report on the use of the personal data during investigation an how to make these reports available to the data subject afterward (if possible in the circumstances

38. Staatscourant, 14 January 2008.

3 Cybercrime investigation and use of data by judicial authorities, limitation by privacy principles

3.1 Cybercrime investigation and the use of personal data for police purposes

Status of Data protection in the Convention on Cybercrime

As we look into Article 14, it states that each party shall adopt such legislative and other measures to establish the powers and procedures provided for in this section (section 2, procedural law) for the purpose of specific criminal investigation. This leaves a great margin of appreciation for the competent authorities. In the light of guarantees for personal data protection, although reference is made as stated hereunder, it is not clear to what level the competence of authorities is limited. In national laws also reference is often made to the fundamental rights and limitation of use of personal data for police purposes.

In Recommendation N° R (87) 15 regulating the use of personal data in the police sector (2002) article 2.1 clearly states that the collection of personal data should be limited to such as is necessary for the prevention of a real danger or the suppression of a specific criminal offence.
Any exception to this provision should be the subject of specific national legislation. The question is to what extent the collection and the use of personal data will be limited.
For instance, there is no clear distinction made between a clear criminal offense and criminal or security investigation and surveillance in more general matters connected to possible dangers. In the case of a clear criminal offender there is already a suspect. This is a narrower definition than general (criminal) investigation where no suspect is identified (yet). One could agree with less guarantees for the obvious suspect. In the latter case it is sufficient to use the procedural and other measures for tracing a criminal offender.
For non-suspect (related) data subject to any (computer) crime it is not acceptable to loose all guarantees on data protection. This (can) concern people (innocent bystanders) who have nothing to do with the perceived crime and investigations whatsoever.

Categories of Data
An other problem could develop in the use of different categories of investigative (police) data. Of course a distinction must be made between sensitive and less sensitive personal data. It seems to be quite logical that data about some body's sexual behaviour must be treated in a more careful and protective way than his address or date of birth

Use of personal data for different purposes and investigations
There could also develop a problem concerning the information that is gathered for the purpose of specific a criminal investigation. The question is if this information is not useable for this specific criminal investigation but is usable for another criminal investigation.
Article 5 of ETS 108 states that personal data undergoing automatic processing shall be adequate, relevant and not excessive in relation to the purpose for which they are stored. Derogation of this article is only possible if this is provided by national law of the party and constitutes a necessary measure in a democratic society in the interests of protecting state security, public safety, and the monetary interests of the state or the suppression of criminal

offences of protecting the data subject or the rights of freedom of others.
As stated above, it must be clear how far the competency of the authorized judicial parties will extend, and what the consequences are for collection, use and preservation of categories of personal data.

Misuse, unauthorized use
Concerning the general risks of misuse, unauthorized us, loss or destruction of personal data Article 7 states that appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss, as well as against unauthorised access, alteration or dissemination. Any exception or restriction of Article 7 is not possible.
What kind of measures are taken to act in conformity of these paragraphs? This includes technical measures as well as procedural security measures as authentication of users, codes etc.
For reasons of security these measures are not publically displayed of course. But how can be controlled if there is conformity with these requirements and how different categories of personal (sensitive) data are treated?

It seems that it is not always clear what the status of personal data is in different phases of in the different national and international regulations.

3.1.1 Defining personal data in the Cybercrime Convention?

Personal data vary in relation to the purpose that is aimed for by collecting the personal data. In Article 2 of the Convention ETS 108, "personal data" means any information relating to an identified or identifiable individual ("data subject"). The Cybercrime Convention refers to ETS 108 but has no specific definition itself, although the Recommendation (87) 15 is applied to be used as such. The expression "for police purposes" covers all the tasks which the police authorities must perform for the prevention and suppression of criminal offences and the maintenance of public order.

For the purposes of the Recommendation, the expression "personal data" covers any information relating to an identified or identifiable individual. An individual shall not be regarded as "identifiable" if identification requires an unreasonable amount of time, cost and manpower.

In criminal procedures (and of course any other data-relevant activity), vast amounts of identifiable personal data are to be processed and have to be considered protectable under privacy regulations. There should be reason to include this to cover any personal data, not only restricted to the persons who are subject of the investigations.

In the Dutch Police Data Act (DPDA) (Wet Politiegegevens), reference is made to the fact that only police data are the subject of this law: the data concerning an identified or identifiable natural person that is processed in the exercise in the police task. There should be a common understanding of the difference between "police data" and "normal personal" data, because of the different levels of protection and treatment.

a. Police-data: any data concerning an identified or identifiable natural person that is being processed in the exercise of the police task;[39]

[39] DPDA, article 1

It must be considered that in this definition, a vast series of data can be considered police data in relation to ongoing investigations and are not treated in the way that "normal" personal data are subjected to protection by general data protection legislation, or even the principles as stated in the scope and definitions of the Appendix to Recommendation No. R (87) 15 although article 4 states that personal data collected and stored by the police for police purposes should be used exclusively for those purposes. Spontaneous information of personal data that is to be used in other ways then it was intended for is not possible under the provision of Article 4.

3.1.2 Defining policy and purpose

The basic principle of (national) policy development concerning the use of personal data and police data, and investigation as such in computer crime, should be based on a more crystallised use of Article 15 CoC, the privacy guarantees of international treaties, independent supervision and reasonable retention of personal data with respect to the interests of the data subjects.[40]

3.2 Police law in cybercrime investigations

In the Cybercrime Convention there is certainly attention to the fact that fundamental rights and freedoms have to be respected. The government is made responsible for implementing the safeguards on the basis of the existing international data protection legislation (art. 15). By implementing the procedural rules as stated in Article 14 of the Cybercrime Convention concerning the scope of procedural provisions, establishing the powers and procedures provided for the purpose of specific criminal investigations or proceedings, as a comparison the Dutch Police Act and the Dutch Code of Criminal Procedures is used. Further, in a more general way these principles are implemented in the privacy laws and other national data protection laws, and other procedural regulations. For reasons of limitation in time and information I will not refer to police legislation in other Member States.

40. Compare in this respect Article 15:
Application of certain provisions of Directive 95/46/EC
1. Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, *inter alia*, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union.
2. The provisions of Chapter III on judicial remedies, liability and sanctions of Directive 95/46/EC shall apply with regard to national provisions adopted pursuant to this Directive and with regard to the individual rights derived from this Directive.
3. The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC shall also carry out the tasks laid down in Article 30 of that Directive with regard to matters covered by this Directive, namely the protection of fundamental rights and freedoms and of legitimate interests in the electronic communications sector.

3.3 Ways of collecting personal data by police investigation, criminal intelligence

Data protection and methods of data collection

In the Netherlands the laws on Police Data refer to Article 9.2 of the European Convention ETS 108, giving the possibility of exception but still referring to the importance of the fair collection principles. For example, in the Dutch Act on Police Data the necessity of investigation has to be made clear in the way that: necessity, lawfulness, purpose specification are to be ensured; police-data will only be processed for as far as is necessary for the defined purposes in this act, which are:

- - the daily execution of the police task (Article 8);
- - targeted research in order to maintain law and order (Article 9 - ongoing difficult cases, involving any person connected);
- - specific research to get information of the involvement of certain people in certain serious threats to the legal order (organised crime) (Article 10);
- - automated comparison (Article 11), between all available police data, on behalf of Articles 8, 9 and 10;
- - crime targeted research
- -Police data will only be processed for as far they are obtained in a lawful manner, and taken in account the purpose for which they are being processed as not being excessive and;
- - as being purpose specific, if a different purpose is used this has to be specified by law;
- -sources and obtainment are to be registered.

As stated in the Evaluation of Recommendation regulating the use of personal data in the police sector by Mr. Patijn, this process is described as a process of criminal intelligence:

> a. Hard data versus soft data. The police data about criminals may vary from (1) data flowing from a well established source to (2) data based on very vague indications about somebody's possible involvement with serious crime. The first category is referred to as hard data, the second as soft data. This last category may even stem from an anonymous source, resulting in complete uncertainty about its trustworthiness. The nature of the information may yet be such that storage, at least for a limited period of time, might be deemed necessary for the proper performance of the police task.[41]

This can be considered as a serious threat to privacy because these mechanisms have increased by:

- "data mining": automated research, analysis and classification of large databases and combining of data to recognise patterns and behaviour and to profile and predict future behaviour;
- interception of electronic communication;
- traditional use of criminal records;
- traditional surveillance.

"Data mining" can be considered an important instrument in fighting crime and threats of conspiracy and terrorism, but is to be exercised with the utmost prudence, so as to

41. Final activity report of the Project Group on Data Protection (CJ-PD), adopted on 28 October 1999.

not to jump to conclusions. However, what presents an even more threatening development is the increasing way of thinking in security preventive policy, where action is taken before a crime is committed or even before somebody can be called a suspect.

As stated in the evaluation:

> As police and judicial powers in most national Codes of criminal procedure are limited to cases where there is a suspicion against a person with regard to a specific criminal offence, new information technology is increasingly used to store data about criminals as persons as such, without relation to specific criminal offences. The data can comprise both soft and hard data, as made explicit above. It does not necessarily meet the standard of a well established suspicion against a person, a standard which must be fulfilled in order to apply the powers conferred on the police in the Code of Criminal Procedure. Nevertheless many countries collect data which may even imply the profiling of the alleged criminal, his behaviour, his contacts and his way of life without much relevance with regard to a specific criminal offence. The data are used to solve any crime, either already committed or expected to be committed in the future.

This unlimited collection of data would be contrary to many privacy principles as stated in this study. It is contrary to the purpose principle and the fact that the action must be proportional etc. Procedures to use this technique have to be clear and transparent and have to be evaluated by an independent authority. This should be provided by law in accordance with Article 9 of the Convention for the protection of individuals with regard to automatic processing of personal data.

It is not always made clear by judicial (or intelligence) authorities on what legal basis the investigation is taking place. Consequently, Internet Service Providers do not always feel very cooperative towards these kinds of investigations:

> In the surveillance society, social sorting is endemic. In government and commerce large personal information databases are analysed and categorized to define target markets and risky populations. In the section on consumer surveillance we shall see how a company like Amazon.com uses sophisticated data mining techniques to profile customers, using both obvious and non obvious relationships between data. [42]

and,

> It wants the data from the search engines to prove how easy it is to stumble over porn on the net. Google's refusal was based on three main arguments. Firstly, Google says it does not want to do the government's work for it and secondly it says that it wants to protect its product. Thirdly, Google wants to show users that the company is serious about protecting their privacy. Cooperating with the government "is a slippery slope and it's a path we shouldn't go down", Google co-founder Sergey Brin told industry analysts earlier this month.[43]

42. Surveillance Report, Surveillance Society, p.8.
43. Zie district court California 3/17/2006

The same accounts for the use of interception techniques: the interception and storage of vast amounts of data have increased by the extension of interception to all kind of electronic communication services, including e-mail traffic and broadcasting techniques.
Comments on the use of data mining by police authorities are not always negative:

> For example, police in Redmond, VA, 'started overlaying crime reports with other data, such as weather, traffic, sports events and paydays for large employers. The data was analyzed three times a day and something interesting emerged: Robberies spiked on paydays near cheque cashing storefronts in specific neighbourhoods. Other clusters also became apparent, and pretty soon police were deploying resources in advance and predicting where crime was most likely to occur.'[44]

Still, police-actions and investigations are not comparable with weather-forecasts and must be exercised with more scruples than that. It should not be allowed to combine and use personal data in these actions however these data are gathered.

3.3.1 Legal powers and procedures adapted to circumstances?

For "traditional" crimes, police authorities have the "normal" ways to carry out investigations as stated above, although the limits of competence are not always taken into account. Since the development of the concept of "terrorist" crimes (after 9/11/2001 and the attacks in London and Madrid), specific investigative powers were developed based on *inter alia* the European Union Council Decision of 19 December 2002 on the implementation of specific measures for police and judicial co-operation to combat terrorism. It stimulated the European member states to:

> (…) designate a specialised service within its police services, which, in accordance with national law, will have access to and collect all relevant information concerning and resulting from criminal investigations conducted by its law enforcement authorities with respect to terrorist offences involving any of the listed persons, groups or entities.
>
> 2. Each Member State shall take necessary measures to ensure that at least the following information collected by the specialised service, is communicated to Europol, through the national unit of that Member State, in accordance with national law and insofar as permitted by the provisions of the Europol Convention, with a view to its processing pursuant to Article 10, and particularly Article 10(6), of that Convention:
>
> (a) data which identify the person, group or entity;
> (b) acts under investigation and their specific circumstances;
> (c) links with other relevant cases of terrorist offences;
> (d) the use of communications technologies;
> (e) the threat posed by the possession of weapons of mass destruction.[45]

This Council decision was further strengthened by the declaration on combating terrorism of March 25 2004 after the attacks in Madrid.

[44] http://yro.slashdot.org/article.pl?sid=07/08/10/1727249
45. Council Decision 2003/48/JHA of 19 December 2002 on the implementation of specific measures for police and judicial cooperation to combat terrorism in accordance with Article 4 of Common Position 2001/931/CFSP, Article 2.

The Council of the European Union issued a vast document stimulating international cooperation against terrorism on a global level, inter alia by stimulating (extensive) legislative measures:

> (a) Legislative Measures
>
> The European Council acknowledges that the legislative framework created by the Union for the purpose of combating terrorism and improving judicial cooperation has a decisive role to play in combating terrorist activities. It urges all Member States to take any measures that remain necessary to implement fully and without delay the following legislative measures:
>
> Framework Decision on the European Arrest Warrant
> Framework Decision on Joint Investigation Teams
> Framework Decision on Combating Terrorism
> Framework Decision on money laundering, the identification, tracing, freezing and confiscation of instrumentalities and the proceeds of crime;
> Decision establishing Eurojust;
> Decision on the implementation of specific measures for police and judicial cooperation to combat terrorism;
>
> Any such measures should be in place no later than June 2004.[46]

3.3.1.1 Terrorist criminal act

Although understandable, it is doubtful if a legal basis for more far-reaching investigative powers is possible without reasonable suspicion whether it concerns a so-called terrorist crime in the Dutch Code Criminal Procedures, i.e.:

> act with a view to terrify the population or a part of the population of a country or to force the authorities or international organisation to act in an unlawful way, or to permit or not permit something or seriously threat to destroy or disrupt the fundamental political ,constitutional or social structure of a country or international organisation.[47]

It is interesting to see that this terrorist act can be directed to any country or international organisation and can therefore be considered a kind of universal crime, not limited to Dutch nationals or territory. In this case, the Netherlands police authorities may act without reasonable suspicion as should normally be required on the basis on the Dutch Code of Criminal Procedures (DCCP)(Article 27 Sv).

3.3.2 Use of "social" or "community" networks to find terrorist threats

The development of social networks, such as "YouTube", "face book", "orkut", etc., gives ample opportunity for investigators to acquire personal information by means of simply

46. Declaration on combating terrorism, Brussels, 25 March 2004. http://www.libertysecurity.org/IMG/pdf/Declaration_EU_anti-terro.pdf
47. Article 83 DCCP
.

logging in to these public or semi-public networks. Because of the character of these networks, there is a vast load of personal information that can be used for profiling subjects. Although this concerns publically available information that can be used by anyone (within the limits of the law), the fact that the police has a purpose specific responsibility would lay a heavier burden on these authorities to use this information with the utmost care and scrutiny.
After the murder of Theo van Gogh and the perceived terrorist attack by the "Hofstad groep" there was much attention by the police for publically available social networks and sites as for instance Maghreb.nl and Marokko.nl

Although in fact this is (at least in part) publicly available information, it is doubtful if it is acceptable that investigative authorities must have the freedom to use this information without the consent or even knowledge of the data subjects, and under further guarantees of Articles 5-9 of ETS 108.

Cooperation by third parties
It is also well known that in the process of collecting (general) information about the (electronic) behaviour of data-subjects requests for information are issued by investigative authorities to third parties.
Not exactly a prototype champion of privacy protection, Google resisted the demand to give insight into the general behaviour and the personal data of its clients to the US justice:

> It wants the data from the search engines to prove how easy it is to stumble over porn on the net. Google's refusal was based on three main arguments. Firstly, Google says it does not want to do the government's work for it and secondly it says that it wants to protect its product. Thirdly, Google wants to show users that the company is serious about protecting their privacy. Cooperating with the government "is a slippery slope and it's a path we shouldn't go down", Google co-founder Sergey Brin told industry analysts earlier this month. [48]

Of course in most General Conditions of ISP's and other personal service providers there is an obligation not to act in unlawful ways or put any illegal contents on their sites or behave in an unlawful way. For instance on Facebook:

> You represent, warrant and agree that no materials of any kind submitted through your account or otherwise posted, transmitted, or shared by you on or through the Service will violate or infringe upon the rights of any third party, including copyright, trademark, privacy, publicity or other personal or proprietary rights; or contain libellous, defamatory or otherwise unlawful material.

Although the Internet provider more or less (General Conditions) prohibits its users to commit unlawful acts when using its service, the Internet providers themselves (and any other person) still have no obligation to inform any authority of illegal acts or content when performing mere conduit and non –content related tasks, there is a tendency that if the provider has knowledge of this (or any) unlawful business he will inform the authorities

48. *Vide district court California 3/17/2006*

3.4 Defining methods of acquiring information and ensuring data protection in regulating criminal investigation

As stated above, there are several general methods of acquiring personal information, by using databases or publicly available sources that need not to apply Articles 16-21 CoC. The ways this information is acquired before it is defined as being "police data" are also described in the "traditional" instruments police authorities have available, as described in Article 126 Code of Criminal Procedures, Special Powers.[49] These powers only can be used in certain circumstances concerning severe criminal acts, especially if it concerns a serious threat to national security of the state, health or security of persons.[50] The most important powers in the Netherlands related to the use of personal data are:

- **Observation:** The authorities have special powers concerning the observation of certain suspects in following and observing his behaviour (126 g DCCP).
- **Systematic gathering of information:** Carried out undercover[51] (also possible by special officers - secret service - or an official of a foreign state!). A special order in writing (by the prosecutor or examining magistrate) is needed, and will only be valid for three months.
- **Wiretapping and other technical devices**: The traditional wiretapping and using of other (conventional) technical devices is covered in Article 126 l DCCP. The "new" developments are covered by Article 126la, a special paragraph on the use of electronic devices for (any other) form of electronic communication, is meant.
- **Search on data storage devices:** In addition, all kinds of electronically processed or stored information can be tapped or obtained, for instance the information from PDA's, in which more and more personal information is stored. Other storage media such as memory sticks and hard disks are also covered by these paragraphs.[52]

In the way information is gathered by the authorities through demand, in case of suspicion of criminal offences, all other participants who have this "identifying" information may also be obliged to hand over this information. This information may consist of NAR (personalia), date of birth, sex and administrative characteristics. These paragraphs give more possibilities to obtain information from different persons and other parties, as well as those parties which are vaguely connected (or not at all) to the suspect, but could be relevant to the case.

It is interesting that in this paragraph reference is made to the fact that this demand cannot be made to the suspect himself but also that the required data may not refer to this persons sensitive personal information concerning somebody's religion or faith, race, political conviction, health, sexual life or membership of a union[53], in accordance with principle 2.4. R.87 (15).

3.4.1 Defining limitations on the research of personal data concerning (cyber) crime

In general it comes to the point where the principles set out in the first paragraph of this study are applicable, and that the investigative activities of the (police) authorities

49. See Also Koops, B.J. a.o, Strafrecht en ICT, (Criminal Law and ICT), SDU, The Hague, 2007, pages 77-122.
50. Article 67a DCCP.
51. Article 126 J DCCP.
52. Article 125 i and j DCCP.
53. Article 126 nc, para. 3 DCCP.

are well enough motivated within the exception of the conditions that for national and international security and judicial activities no real description of this motivation is given in law or in policy.

3.4.2 The identification *of targets of criminal intelligence*

Under paragraph 5.2.1 of the evaluation report it is stated that

> Not everybody can indiscriminately become the subject of criminal intelligence, the law must define the criteria for identifying the targets that can be the subject of criminal intelligence. These criteria will differ according to national law and can be criteria based on content or on procedure. Criteria based on content are, for example, the restriction to gather criminal intelligence only in cases of serious organised crime and crimes of a comparable threat to society. A criterion based on procedure is for instance that a Ministry of Justice, a Ministry of Internal Affairs, a judge or a public prosecutor, mandating the collection of criminal intelligence during a limited period of time and, if possible, within a geographically defined area about a precisely defined group of persons who are suspected of being involved or becoming involved in a specifically circumscribed area of crime. The question then to be answered is whether the mandate should be a publicly available document, either from the very beginning, or as soon as possible if the investigation can no longer be jeopardised.

In the Dutch Law on Police Data (Wet op Politiegegevens[54]) no specific provision is made for the data subject as a target for criminal intelligence. The data subject is defined as the person concerned to whom the police data relates,[55] in a very broad sense. Almost any data in police investigation is considered as such. Any person that is in one way or another connected to this investigation will be not protected according to the "normal' principles of data protection. The question is if "guaranteed" by law as stated in the exception of article 6 jo. Article 9 of ETS 108 will apply to such "umbrella" definitions.

3.4.3 Other instruments regulating data

In the European Union Context there is a draft framework decision on the handling of data in police matters[56]The Framework Decision applies only to data gathered or processed by competent authorities for the purpose of the prevention, investigation, detection or prosecution of criminal offences, or the execution of criminal penalties. The Framework Decision leaves it to member states to determine more precisely at national level which other purposes are to be considered incompatible with the purpose for which the personal data were originally collected. In general, further processing for historical, statistical or scientific purposes is not incompatible with the original purpose of the processing.

3.5 The matching of data from open sources, such as the Internet or public files and telecom traffic

54. Act of 21 juli 2007, rules concerning the processing of police data (houdende regels inzake de verwerking van politiegegevens) (*Wet politiegegevens*)
55. Article 1 g.subject, the person on whom the policedata are applicable (betrokkene: degene op wie een politiegegeven betrekking heef)t;
Coreper, Council of the European Union, Inter institutional File: 2005/0202 (CNS [56]

As stated above under sections 3.3 and 3.4, judicial authorities have been given competencies to search any databases in national legislation (Articles 16-21 CoC). Although public available data can also be used, it should be dependent on the purpose of the search and should be described as far as possible in the court order. This kind of data-searching is not necessarily documented in investigational reports but should be documented in the official registration document (proces verbaal)

In the Cybercrime Convention and cited national law, the preservation of stored computer data is considered a legitimate way to obtain information about offences and is expected to include traffic data from telecommunication as well.

Any kind of third party can be ordered to preserve (and deliver) data to the competent criminal authorities (Article 17 CoC) and preserve and make any data available for 90 days, whatever the source (operator) may be.

3.6 Retention of data and purposes in the investigative process

For investigative authorities there were already ample opportunities to acquire data and hold them for 90 days (Article 16 CoC and Article 126 ni DCCP), but as stated above, the Retention Directive gives the possibility to increase the competence on time limit and contents.

A recent trend is also that legislation is passed to *mandate* the storage and processing of data, for fear of the data disappearing before they can be used by the government for law enforcement or national-security purposes. Examples are the preservation order (Article 16 Cybercrime Convention, implemented in Article 126ni, 126ui, 126zja DCCP, and the Data Retention Directive (2006/24/EC), which mandates telecom providers to store all traffic data for a period of six months to two years (a Dutch implementation Bill is currently pending in parliament). These data, stored for government purposes, may then also be used by the private parties storing them, and perhaps be shared with other third parties as well, as long as they comply with the relevant legal framework for data processing (like the Data Protection Act and Chapter 11 of the Telecommunications Act).

Almost all of these data, both the 'emerging' data and those mandatorily stored, can, if legal conditions are met, be accessed and used by the government for law-enforcement and intelligence purposes. Both the judiciary and the intelligence services have comprehensive powers to order delivery of data or to gather data themselves. The question can be posed if this is not going beyond the purpose as stated in Article 16.

3.7 Storage and destruction of data

In the Retention Directive (3), Articles 5, 6 and 9 of Directive 2002/58/EC lay down the rules applicable to the processing by network and service providers of traffic and location data generated by using electronic communications services. Such data must be erased or made anonymous when no longer needed for the purpose of the transmission of a communication, except for the data necessary for billing or interconnection payments.

Article 15(1) of Directive 2002/58/EC sets out the conditions under which member states may restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of that directive. Any such restrictions must be necessary, appropriate and proportionate within a democratic society for specific public order purposes, i.e. to safeguard national security (i.e. state security), defence, public security or the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communications systems.

The provisions in R 87. 15 provide in principle 2 for the use of data as long is necessary for the purpose. National legislation has to provide for the implementation of guarantees against misuse. If not useful for its purpose the data have to be removed. It is doubtful that the data subject will be informed about use and retention, as stated in principle 2.2.

3.8 (Democratic) control mechanisms

In general, the control mechanisms on day-to-day use of police powers are more or less formal. In the Netherlands, as certainly in other democratic societies, the responsible ministers, Justice Department and Interior, can be held responsible by parliament for their policy and execution of formal and executive tasks and used instruments. For the control on privacy laws as such the role of the DPA and the ultimate responsibility of the Minister of Justice in this respect is clear as well.

The fact is, however, that one vision of our democratic (western) society is shifting concerning the values of personal freedom and privacy in comparison with the value of security of society. I have given several examples of this in the foregoing text.

In the Converging Technologies Report[57] this is explained by the shift that has taken place in the rethinking of the purpose of criminal law and policy as such:

> Recently, the attention seems to shift to interests of society, deterrence and retribution. Converging technologies have the potential of reorganising the fight against crime and terrorism. Rather than being restricted to damage control – finding and punishing perpetrators – damage *prevention* becomes a focus for law enforcement.

This shift means that it is widely accepted that control of society is not considered a dirty word anymore and that even parliament, being a mirror of the society, will control under the premises of the importance of the control of society to enforce security. As the former Dutch Minister of Justice, now Minister of Social Affairs, Donner, stated in a discussion program on Dutch television concerning the influence of the Islam on society: "if two thirds of Dutch society agrees upon the introduction of the Sharia and abandoning of Democracy, this is a valid democratic decision."[58]

It is equally important to remember the point about the corruptions and skewed visions of power. Again, we do not have to imagine some wicked tyrant getting access keys to social security or medical databases to see the problem. The corruptions of power

57. CTR, page 116.
58. Dutch television, "Paul en Witteman", 13 September 2007.

include leaders who appeal to some supposed greater good[59] (like victory in war) to justify unusual or extraordinary tactics.

Also in Germany there is considered to be a downward directed spiral of fundamental rights loosing points to protection against pertained security risks and enhancing measures to give non-democratic solutions precedence. The German Minister of Interior tried to establish database searches against terrorist perpetrators on a European level, after his national attempts turned out a total failure in order to push the national discussion using the power of the European Council. Similar efforts can be determined – by the European Council – for the Cybercrime Convention. This procedure is much more obvious concerning stock of telecommunication traffic data; the German Minister of Interior switched to the European level after recognising that the Bundestag (Federal Parliament) would not be willing to support his political demands. The idea is to force the national legislator by European law to pass a national law that otherwise would not have been passed at all. Such procedures can be called "policy laundering".

This tendency is encouraged by what seems to be a reduced standard in fundamental rights on a European level. The jurisdiction of the Federal Constitutional Court (Bundesverfassungsgericht), which explicitly stresses basic constitutional rights, must not be taken directly into consideration by EU-bodies, especially the European Council, when reaching consent on intrusions on privacy rights.

Recognizing the fact that it is almost impossible to control national security Agencies, it was time for the Germans to set a (new) standard: National secret services agencies are only permitted to (clandestine)monitor the computers of people suspected of crimes or terrorism if they have evidence showing the suspects are dangerous in a way that there is considered a concrete threat to human life or the State

Further it is decided that the "Constitutional General Personality right" evidently also encompasses the confidentiality and integrity of information technology systems:

59. *A Report on the Surveillance Society* For the Information Commissioner by the Surveillance Studies Network September 2006, page 2.

The constitutionality of online searches of electronic information systems in Germany

On 27 February 2008 the First Senate of the Federal Constitutional Court of Germany declared in its judgment that a provision of the law on the intelligence service in the State of North Rhine Westphalia of 20 December 2006 was not compatible with the German Constitutional Law. The provision permitted the covert observation of the Internet and moreover covert access to technical information systems. It has been the first and only regulation in Germany so far that explicitly authorized covert online searches.

In its judgment the Constitutional Court formulated a new basic right, namely the right to the confidentiality and integrity of technical information systems, and ruled that intrusions into this right are only justified in very specific circumstances which must be clearly defined by law. It can be anticipated that this ruling will influence the development of future regulations of online searches not only in Germany but also other countries.

Judgment of the First Senate of the Federal Constitutional Court of Germany of 27 February 2008 – Guiding principles[60]

1. *The general personality right (Art. 2 Abs. 1 in association with Art. 1 Abs. 1 GG[61]) comprises the basic right of having the confidentiality and integrity of technical information systems ensured.*
2. *The covert infiltration of a technical information system through which the use of the system can be surveyed and its storage media read, is constitutionally only admitted, if there are actual criteria for a concrete threat to a paramount legally protected interest. Of paramount importance are life, limb and freedom of the person or such interests of the general public the threat to which affects the survival of the State or the basis of the existence of people. The measure may be justified already then, when it is not yet possible to determine with sufficient probability that the danger will occur in the near future, as long as specific facts in a concrete case point at the dangerous threat by specific persons to the paramount protected legal interest.*
3. *The covert infiltration of a technical information system is as a principle subject to a judicial order. The law authorizing such a measure, must contain provisions to protect the core area of the private conduct of life.*
4. *In so far as an authorisation is limited to a measure by the State through which the contents and context of the ongoing telecommunication in a computer network are intercepted or related data is analysed, the measure is to be seen against Art. 10 Abs. 1 GG.[62]*
5. *If the State obtains knowledge of the contents of Internet communication in the manner technically foreseen, it constitutes an intrusion into Art. 10 Abs. 1 GG only if the State body has not been authorized to take note by participants in the communication.*

---

[60] Quote: BVerfG, 1 BvR 370/07 vom 27.2.2008, Absatz-Nr. (1 - 333), http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html
Inofficial translation. Footnotes added for ease of reference.

[61] German Basis Law (constitution):
Article 1
[Human dignity]
(1) Human dignity shall be inviolable. To respect and protect it shall be the duty of all state authority.
(2) The German people therefore acknowledge inviolable and inalienable human rights as the basis of every community, of peace and of justice in the world.
(3) The following basic rights shall bind the legislature, the executive, and the judiciary as directly applicable law.
Article 2
[Personal freedoms]
(1) Every person shall have the right to free development of his personality insofar as he does not violate the rights of others or offend against the constitutional order or the moral law.

[62] **Article 10**
[Privacy of correspondence, posts and telecommunications]
(1) The privacy of correspondence, posts and telecommunications shall be inviolable.
(2) Restrictions may be ordered only pursuant to a law. If the restriction serves to protect the free democratic basic order or the existence or security of the Federation or of a Land, the law may provide that the person affected shall not be informed of the restriction and that recourse to the courts shall be replaced by a review of the case by agencies and auxiliary agencies appointed by the legislature.

If the State obtains the contents of publicly available communications or participates in publicly accessible communications, he does not as a matter of principle interfere in basic rights.

This means, at least in Germany that "Länder" law on competencies of investigative authorities has to take in account the confidentiality and integrity of personal data on (secured) internet communication and data files on PC,s and any other data file that is not available publically.

4 Overview of activities in an international perspective

4.1 Exchange of personal data by police across borders

4.1.1 The Prüm Treaty

In reaction to terrorist threats, on 25 May 2005 seven EU Member States signed an agreement in the German city of Prüm. The Treaty of Prüm is a treaty of international law, adopted outside the framework of the European Union, but from the content-side closely related to the EU and even with the aim of incorporating the provisions of this Convention into the legal framework of the European Union (Article 1.4).[63]

The Treaty establishes a legal framework to further develop co-operation among member states in combating terrorism, cross-border crime and illegal immigration. More specifically, it provides for the exchange between the Contracting Parties of data on DNA, fingerprints, vehicle registration, and personal and non-personal data related to cross-border police co-operation. The Hague Programme[64] sets 1 January 2008 as the date as from which the exchange of data should be based on the principle of availability. This means that a law officer in one member state who needs information in order to pursue his duties can obtain this information from another member state (the information will be made 'available').

It is the intention of the European Union to enhance information exchange. It could be discussed if the Prüm Treaty undermines the democratic European decision-making process in the area of security and the "availability" programme. But it seems that the possible integration of "Prüm" is considered.

In a reaction by the Rapporteur Fausto Correia, in a working document to prepare for the possible integration of the treaty in the European Union Legal framework, he states that:

> The Treaty of Prüm was negotiated and adopted in a very non-transparent way and without serious democratic control (national parliaments are only involved at the stage of the ratification and the European Parliament is only now involved by means of consultation on the draft Council Decision). Although the Treaty of Prüm states in its Article 1(4) that: "within three years at most following entry into force of this Treaty, on the basis of an assessment of experience of its implementation, an initiative shall be submitted, in consultation with or on a proposal from the European Commission, in compliance with the provisions of the Treaty of the European Union and the Treaty establishing the European Community, with the aim of incorporating the provisions of this Treaty into the legal framework of the European Union" a draft Council Decision is already now presented.[65]

The rapporteur considers the incorporation into the EU framework as a very good step, because it contributes to transparency and legal certainty, however, it is regretful that only parts of its content (namely the issues related to the Third Pillar) are currently

63. Convention between the Kingdom of Belgium, the Federal Republic of Germany, the Kingdom of Spain, the French Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands and the Republic of Austria on the stepping up of cross-border cooperation particularly in combating terrorism, cross-border crime and illegal migration, Prüm (Germany), 27 May 2005, Council Secretariat, Brussels, 7 July 2005, 10900/05.
64. The Hague Programme for strengthening Freedom, Security and Justice in the EU approved by the European Council on 5 November 2004.
65. Rapporteur: Fausto Correia, 10.04.2007, Working Document on a Council Decision on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, Committee on Civil Liberties, Justice and Home Affairs.

proposed to be incorporated. He thinks it is of utmost importance that: "the proposed measures should be necessary and proportionate. Also, mechanisms of evaluation control and redress should be foreseen in order to correct problematic situations." Furthermore, he is doubtful about the substantial requirements for accessing personal data and the fact that there is no real harmonisation on procedures.

4.1.2 Protection of data in police matters

On 4 October 2005 the European Commission forwarded a proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.[66] The last commented proposal is of November 2007.

> Its third Consideration states where it stands for:
> In it, legislation falling within the ambit of Title VI of the Treaty on European Union should foster police and judicial cooperation in criminal matters with regard to its efficiency as well as its legitimacy and compliance with fundamental rights, in particular the right to privacy and to protection of personal data. Common standards regarding the processing and protection of personal data processed for the purpose of preventing and combating crime can contribute to achieving both aims.

As a principle this seems to be a good start, but in the Declaration adopted by the European Data Protection Authorities[67] they state (of course) that "it is evident that any development in this area must be balanced with adequate and harmonised data protection rights and obligations in which mutual trust is a key element". They are not satisfied with the good intentions of the European Commission and stress that the scope of the proposed framework decision should apply to all processing activities by police and judicial authorities to give individuals the necessary protection.

4.1.3 Interpol, Europol

Interpol collects, stores, analyses and exchanges information about suspected individuals and groups and their activities. The organisation also co-ordinates the circulation of alerts and warnings on terrorists, dangerous criminals and weapons threats to police in member countries. A chief initiative in this area is the Fusion Task Force, which was created in the aftermath of the 11 September attacks in the United States.

Interpol has been actively involved for a number of years in combating Information Technology Crime. Rather than 're-inventing the wheel', the Interpol General Secretariat has harnessed the expertise of its members in the field of Information Technology Crime (ITC) through the vehicle of a 'working party' or a group of experts. In this instance, the working party consists of the heads or experienced members of national computer crime units. These working parties have been designed to reflect regional expertise and exist in Europe, Asia, the Americas and in Africa. All the working parties are in different stages of development. It should be noted that the work done by

66. Coreper, Council of the European Union, Inter institutional File: 2005/0202 (CNS).
67. Spring Conference of European Data Protection Commissioners
http://www.garanteprivacy.it/garante/doc.jsp?ID=1408346 (document in Italian).

the working parties is not Interpol's only contribution to combating ITC, but it certainly represents the most noteworthy contribution to date.

Europol is the Police Office of the European Union that handles criminal information. Its mission is to assist the law enforcement authorities of member states in their fight against serious forms of organized crime whilst fully respecting human rights. Europol's main tasks are to facilitate the exchange of information between member states and to provide analytical expertise.

The Europol Convention provides for the creation of a Joint Supervisory Body[68] – an independent body with the task of ensuring Europol's compliance with data protection principles. The JSB reviews all activities of Europol in order to ensure that the rights of the individual are not violated through the storage, processing and utilisation of their data held by Europol. It also monitors the permissibility of the transmission of data originating from Europol. Each individual has the right to request the Joint Supervisory Body to ensure that the manner in which his personal data have been collected, stored, processed and utilised by Europol is lawful and accurate. The Europol Convention establishes the Appeals Committee of the Joint Supervisory Body which is charged with examining appeals of Europol's decisions by all appropriate means. The Appeals Committee is independent and impartial and not bound by directives of the JSB.

Since the Treaty of Amsterdam committed member states to create "an area of freedom, security and justice", one of the EU's key objectives was to improve co-operation between law enforcement authorities. The goal of constructing an "Area of Freedom, Security and Justice" across the Union was agreed on at the 1999 EU Summit in Tampere. The 'Tampere programme' was a five-year agenda that came to an end in 2004.

In June 2004, the European Union followed up the Tampere programme by setting future guidelines for a new justice and home affairs agenda for the coming years. A new programme for justice and home affairs, known as the 'Hague Programme' was adopted. The Hague programme is a five-year programme for closer co-operation in justice and home affairs at the EU level between 2005 and 2010. It aims to make Europe an area of freedom, security and justice. The programme promotes the development of adequate safeguards and of effective legal remedies for the transfer of personal data for the purpose of police and judicial cooperation in criminal matters.

These programs seem to be rather high level and give no indication of control mechanisms, for instance in the procedural requirements in international assistance or "spontaneous" information as referred to in Articles 25 and 26 CoC.

Still, criminal procedures, surveillance, investigation and enforcement procedures are considered national competence areas. In the aforementioned study of the Telematics Institute, the following examples are to illustrate the practical developments in this area.

Although, for instance, the influence of the EU on member states' criminal law systems is increasing, nations are still reluctant to hand over responsibility for law enforcement

70. The Third Activity Report of the Joint Supervisory Body of Europol, Nov 2004 – Oct 2006, http://www.cbpweb.nl/downloads_int/EUROPOL_Activityreport_3_EN.pdf?refer=true&theme=blue

to a supranational level. For applications in converging technologies, this means that often, for each new application in the sphere of law enforcement, discussions have to take place and agreements have to be made among EU member states for facilitating cross-border use. Mutual access to DNA profiles in national forensic databases (cf. the Prüm Convention), cross-border computer network searches (cf. the Convention on Cybercrime), and technical protocols for wiretapping (cf. the ETSI ES 201 671 and ETSI-NL standardisation procedures) are examples that illustrate how slow, complex, and piecemeal such supranational discussions and decision-making are. For applications like crowd control based on RFID tags (pre-crime scenario) or prisoner-tracking through GPS (social crime control scenario), this means that such applications will likely be restricted to the national context first, reducing their effectiveness, and that cumbersome procedures will have to be followed to enable cross-European applications.

In Europol the key measures aim to make police information available for all law EU enforcement authorities and to improve the use of Europol.

The programme also stresses the need to establish adequate data protection rules. This is in line with the European Parliament's call for harmonised data protection rules under the Third Pillar, whilst guaranteeing the same data protection level as under the First Pillar.

At the 2005 "Spring Conference of European Data Protection Authorities" the need was discussed for closer co-operation between the EU's law enforcement authorities and those of third states, and the need for adequate data protection. The European Data Protection Authorities concluded that the 1981 Council of Europe Convention on Data Protection (Convention 108), applicable in the Union and in member states, was too general to effectively safeguard data protection in the area of law enforcement. It was held that some initiatives to improve law enforcement in the EU, such as the availability principle, should only be introduced on the basis of an adequate data protection system that ensured a high and equivalent standard of data protection.

As recalled before, in 2005 the European Commission submitted a proposal for a Council Framework Decision on the Protection of Personal Data processed in the framework of police and judicial cooperation in criminal matters. However, this proposal excluded Europol from its application.

Another development was initiated by the Austrian presidency. After evaluating the role of Europol, various initiatives were launched for further discussions on its role and tasks. The Joint Supervisory Body was actively involved in these discussions.

The question is if the co-operation actually improves, what kind of guarantees are given to secure the personal information and if the principles of purpose and proportionality are sufficiently taken into consideration.

Principle 5.4 R (87) 15 gives clear provisions when communication of data between foreign authorities is possible; the communication should only be restricted to police bodies. It is only permissible if there exists a clear legal provision under national or international law. Is Article 26 CoC a clear legal provision? If this is not the case, it is only permissible if the communication is necessary for the prevention of a serious and imminent danger or for the suppression of serious and imminent danger comparable with the decision of the German Constitutional Court.

4.1.4 Other actions, echelon, etc.

It is not surprising that not all actions by national and international authorities in obtaining personal data are governed by openly and democratically controlled procedures. Certainly in the field of "national intelligence" the protection of fundamental rights and privacy is not the first objective. In the co-operation between certain national intelligence agencies, democratic control seems to be rather naïve wishful thinking.

In its considerations, the committee[69] is already speaking out over its doubts about the combination of privacy protection and interception:

> Whereas any interception of communications represents serious interference with an individual's exercise of the right to privacy; whereas Article 8 of the ECHR, which guarantees respect for private life, permits interference with the exercise of that right only in the interests of national security, in so far as this is in accordance with domestic law and the provisions in question are generally accessible and lay down under what circumstances, and subject to what conditions, the state may undertake such interference; whereas interference must be proportionate, so that competing interests need to be weighed up and, under the terms of the case law of the European Court of Human Rights, it is not enough that the interference should merely be useful or desirable.

This is considered in violation with the proportionality principle. Furthermore, the committee has severe doubts of the existence of a valid legal basis.

The situation for European citizens in Europe is unsatisfactory. The powers of national intelligence services in the sphere of telecommunications surveillance differ very substantially in scope, and the same applies to the powers of the monitoring committees. Not all those member states which operate an intelligence service have also set up independent parliamentary monitoring bodies endowed with the appropriate supervisory powers. A uniform level of protection is still a distant objective.

On top of that there is pressure coming from the other side of the Atlantic Ocean not to be too conscious about data protection principles considering the application of the contents of article 25.2 of EC Directive 95/46/EC:
2. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.

> **EU-USA: NEGOTIATING AWAY EU DATA PROTECTION**: The EU and USA are negotiating in a secret committee - High Level Contact Group - to come up with a proposal covering data protection in *all future exchanges* of personal data to the USA. To this end they are discussing: **Data Protection**

69. European Parliament, Temporary Committee on the ECHELON Interception System 11 July 2001, report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098(INI)), p. 95.

principles for which common language has been developed (EU document, pdf). Paul Rosenzweig, Deputy Assistant Secretary for Policy at the US DHS said, in November 2007, on the EU requirement that data can only be passed to third states whose laws passed the "adequacy" test guaranteeing equivalent rights: *"The EU should reconsider its decision to apply notions of adequacy to the critical area of law enforcement and public safety. Otherwise the EU runs the very real risk of turning itself into a self-imposed island, isolated from the very allies it needs"* (Privacy and Security Law) He is also opposed to the EU's draft Framework Decision on data protection in police and criminal matters (covering the exchange of personal data *within* the EU), on this: *"The draft seeks to apply the same tired, failed standards of adequacy that it has applied in its commercial laws." [EC Directive 95/46/EC)* The 1974 US Privacy Law gives no protection to non-US citizens, from the EU or elsewhere.[70]

4.2 Codes of police conduct and procedures

In general, there are no compulsory regulations except for what is regulated in the law itself as the DCCP in the Netherlands. There are, however, codes of conduct as to how police and the general prosecution have to behave. Concerning privacy and criminal procedures in the Netherlands, in the Code of Conduct of the Prosecution (Gedragscode Openbaar Ministerie)[71] it is mentioned that the officials will behave in accordance with national and international standards and more specifically with respect for all fundamental human rights, human integrity, with consideration for subsidiarity and proportionality[72] in their task, etc.

The UK police also is bound to a published code of conduct in which, among others, confidentiality of personal information is held high.[73]

In general one could say that codes of conducts have no extra dimension and are on too high a level to be of influence on the actual implementation of fundamental rights and more specific privacy on police procedures.

4.3 European supervision on harmonisation of procedures

The existing instruments are hesitant towards real supervision because of the principle of national sovereignty at the subject of security and criminal investigations. In the EDPC report it was recommended that considering a framework of data protection in the case of availability there is a recommendation for supervision, but it is doubtful that this will be accepted by the participating states:

[70] http://it.slashdot.org/article.pl?sid=07/07/12/2119213
[71] Code of Conduct of the Prosecution(Gedragscode Openbaar Ministerie Vastgesteld door het College van Procureurs-Generaal op 11 juli 2005)
[72] The employee of the prosecution perform their tasks*:*
- within the boundaries of the law;
- with special attention for the fundamental human rights;
- with respect for the human dignity without any discrimination concerning person or status, religion, sex, sexual orientation, nationality, etnicity, colour of skin, age or any other element;
- fair, unpartia,l objective and fearless;
- in a way that will be controlable afterwards and for which choices and decisions that are made people can be held responsible; d;
- with taking into account the rules of proportionality and subsidiarity;

73. Information which comes into the possession of the police should be treated as confidential. It should not be used for personal benefit and nor should it be divulged to other parties except in the proper course of police duty. Similarly, officers should respect, as confidential, information about force policy and operations unless authorised to disclose it in the course of their duties, www.policeuk.com/study/codes.html

> Supervisory authorities: the concept of a JSA shall be understood as an independent supervisory authority. The framework decision shall provide for its composition, tasks and competences. It shall be endowed in particular with consultative, investigative and intervention powers.[74]

As stated above in the case of Europol, the JBS could co-ordinate its role with JSA, but seeing the difficulties in international cooperation this might be hard to imagine. Co-operation between independent supervisory authorities, as stated in Article 2.2. of R (15) 87, would be even harder to imagine.

74. Declaration adopted by the European Data Protection Authorities, Larnaka, 10-11 May 2007.

5 Conclusive remarks and recommendations

The Netherlands' Minister of Justice, Hirsch Ballin, stated on 30 November 2007 that security and privacy are equally codified in Articles 5 and 8 of the ECHR, not being absolute rights, but open to interference of authorities when needed.[75]

The effect of (terrorist) cybercrime can span the globe and one could argue that therefore harsher measures and extended competencies are a necessity. The complexity and thus the difficulty in defining "new criminal acts" may stand in the way to provide a clear description of the criminal conduct, its effects and the (number of) perpetrators.

As stated by Ulrich Sieber:

> The new risks are combined with a high complexity of offences that do not rest on technical or scientifical causes, but on specific perpetrator structures , a high number of victims or a high geographical expansion and extensiveness of the perpetration of the crime. [76]

Considering the field electronic (supported)_ crime and national security and the instruments for investigation, one could conclude that there is no clear distinction and description anymore in criminal acts, criminals and other (connected) persons. How to apply criminal law in such circumstances? Sieber speaks of the "de-limitation of criminal law and new security law" (Entgrenzung des Strafrechts und neuen Sicherheitsrechts"), a dangerous development for the enforcement of fundamental human rights and more specific privacy.

When neither the suspect nor the criminal act have to be specified and criminal law develops into a kind of prevention law the nature of penal law, the most far-reaching intrusion by national authorities in personal life, criminal law, may be without any guarantee and control of society and would be hardly to discern from legal systems that govern dictatorial states.

> Computerworld reports that the FBI is using data mining programs to track more than just terrorists. The program's original focus was to identify potential terrorists, but additional patterns have been developed for identity theft rings, fraudulent housing transactions, Internet pharmacy fraud, automobile insurance fraud, and health-care-related fraud. From the article: 'In a statement, Sen. Patrick Leahy (D-Vt.), chairman of the Senate Judiciary Committee, said the report [on the data mining] was four months late and raised more questions than it answered. The report "demonstrates just how dramatically the Bush administration has expanded the use of [data mining] technology, often in secret, to collect and sift through Americans' most sensitive personal information," he said. At the same time, the report provides an "important and all-too-rare ray of sunshine on the department's data mining activities," Leahy said. It would give Congress a way to conduct "meaningful oversight" he said.'"[77]

75. http://www.justitie.nl/actueel/toespraken/archief-2007/71101privacy.aspx?cp=34&cs=581
76. Ulrich Sieber, Grenzen des Strafrechts, ZStW (2007) Heft 1, p.25.
77 http://it.slashdot.org/article.pl?sid=07/07/12/2119213

Before our world slips into a kind of "minority report" we have to rethink the effects of elastic criminal law. What to do?

In trying to retain some respect for and application of fundamental rights and more specific privacy, it is necessary to at least respect the fundamental principles in the process of surveillance and criminal procedures. As cited in this report in the human rights conventions and latest in the comments of the national data protection authorities, when considering a framework of data protection, it should be stressed that in police and judicial activities, the Working Party on Police and Justice (nominated by the Conference of European Data Protection Authorities), observes that the principles of Convention 108 cannot be surpassed[78]:

> The European States committed themselves to fully complying with Council of Europe Convention 108 of 1981 whose binding principles also cover the activities in the police and law enforcement field. Those principles were subsequently complemented by the adoption by the Committee of Ministers of a specific Recommendation (R (87) 15) regulating the use of personal data in the police sector, and by two Additional Protocols... [and] it is especially urgent to ensure that the level of protection to be afforded should not be lower than that currently set out in the existing and binding legal instruments.
>
> The WPPJ stresses that for certain aspects the current text of the proposal does not provide for the same level of protection as defined in Convention 108. This certainly seems to be the case with the provision on the further use of data received from a Member State (Articles 3 and 12) and the right of access (Article 17).

These articles concern proportionality and purpose and most crucially the fact the individual will only have access to the data held on them (subject to many exceptions) if they make a formal request (Article 12) rather than being informed automatically that data on them is being processed and further transmitted.

It is defendable that new crimes demand new competencies, but procedural principles in personal data protection can be honoured without hampering the work of inter(national) authorities. Therefore it is recommended that at least the following principles[79] in the processing of personal data in criminal procedural activities, be it cybercrime or other "new" criminal behaviour, are to be applied by police and judicial authorities. If not implemented in (inter) national law, comparable principles should be laid down in codes of conduct.

It is advisable to state clearly the principles that are applicable on the processing of personal data as described, *inter alia,* the Cybercrime Convention and the availability proposals and national law in more specific ways than general reference to international human right conventions and henceforth should oblige the investigative authorities to handle accordingly.

It is certainly necessary to distinguish the competencies of judicial authorities in pre-investigative processes , processing and using personal data of data subjects in the different phases of the surveillance, investigation and actual criminal proceedings.

78. Comments from EU Data Protection authorities to the Portuguese Council Presidency on the draft Framework Decision on personal data in police and judicial issues, http://www.statewatch.org/news/2007/nov/eu-dp-wppj-statement-on-dpfd.pdf

79. Derived from this study and the proposal made by the National Privacy Authorities in Spring Conference of European Data Protection Commissioners, Larnaka (Cipro), 10-11May 2007, cf. note 49.

It can not be true , that a clear criminal suspect whereas it concerns the processing of his personal data in a criminal proceeding will be treated in the same way as non-suspect data subjects in data mining and judicial ”fishing expeditions”.

Considering the actions of criminal investigative authorities in the research, use or processing of personal data, it is only allowed to act according to the following principles:

- **Fair collection principle**: personal data should be gathered by fair and lawful means
- **Proportionality** (**minimality) principle**: the amount of personal data gathered should be limited to what is necessary to achieve the purpose(s) of gathering the data;
- **Clear description principle**: the criminal behaviour or act or connection of the concerned subject has to clearly described in the Code of criminal law and considered clearly applicable by accountable criminal or judicial authorities before processing his personal data
- **Purpose specification**: personal data should be gathered for specified and lawful purposes and not processed in ways that are incompatible with those purposes without maintaining any general clause allowing for further processing "for any other purposes".
- **Information of the data subject:** Information of the data subject shall provide for complete provisions including the identity of the data controller, the possible recipients and the legal basis for processing. Any restrictions shall be precise and limited and based on law.
- **(Sensitive) Data categories:** the processing of special categories of data is prohibited unless specific conditions are met and specific guarantees are foreseeing in the national legislation (conforms to Article 8 EU Directive, Article 6 Convention 108). Furthermore, appropriate safeguards shall be provided for the processing of biometric and genetic data.
- **Categories of data subject:** It is a requirement of the principle of proportionality to reintroduce distinctions between the different categories of data subject concerned by the processing for police and law enforcement purposes
- **Accountability principle:** authorities responsible for processing personal data should be accountable for complying with the above principles. Subject should have the means to hold these authorities responsible accordingly. Therefore all actions of investigative authorities must be registered, including data research, retention and involved third parties.

Further, with reference to the advice of the Data Protection Commissioners, the following requirements and rights have to be taken in account:

- **Regulation of data transfers to third countries:** It is a requirement of the adequacy principle that common criteria and a procedure for the adoption of the measures necessary in order to assess the level of data protection in a third country or international body is defined before transferring the personal data and not leave it entirely to the discretion of Member States. Fixing an (common) (EU) standard in such a procedure is a requirement for achieving harmonisation in Europe and the concept of adequacy findings corresponds to the provision in the Council of Europe Convention of 28 January 1981 for the protection of Individuals.
- **Right of access:** the regime of the right of access must be in line with the requirements of the European Human Rights Convention and the case law. In excluding in some cases the possibility to have an effective right of appeal, (…) Furthermore the supervisory authorities or appeal jurisdiction shall have the right to

communicate information to the data subject in case of unjustified refusal. The exception to the right of access shall be (as) limited (as possible).

- **Notification and prior checking:** notification and prior checking of processing to the supervisory authority should, where appropriate, constitute a precondition for processing. Prior checking shall be carried out by the national data supervisory authorities. The possibility of exemptions from publication of notification will have to be considered according to the nature of processing.

Privacy protection to what extent?

The difficult question remains whether states always retain and must exercise the right to breach privacy rights in case of national security, i.e. unlimited powers by national intelligence agencies.[80] This also accounts for measures against (computer related) child pornography where general skim[81] activities are used to discover (potential) criminals. There is a different regime for the protection of personal data in for instance infringements of copyright and related rights (Article 10 CoC) compared to child pornography (Article 9 CoC).
Also there is the problem that there is a difference in interpretation of the texts of the CoC: In 2.c the term: *realistic images representing a minor engaged in sexually explicit conduct.* is translated in Dutch law as: "realistic images, *that cannot be distinguished from reality*"[82] This could create problems if this act is considered to be a crime in one country but not in an other CoC Member State.
And where are the limits in giving each other mutual assistance in this matter if there are different perceptions of the criminal character and punishability of the same act ?
Article 25 CoC provides principles relating to mutual assistance. Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.
Principle 4 R (87) 15 states that personal data collected and stored by the police for police purposes should be used exclusively for those purposes. So if mutual assistance is requested that concerns personal data and will be used for other purposes than it was collected and stored for this request, should this request be denied? Does it derive from this article that parties cannot give mutual assistance to the widest extent possible?

---

80. EU doc no: 13496/07, http://www.statewatch.org/news/2007/oct/eu-dp-13496.pdf
This latter document sets out "five political questions" for decisions within the Council. These include inserting a clause saying that: *"This Framework Decision is without prejudice to essential national security interests and specific intelligence activities in the field of national security."* (Art 1.4). Apparently "all delegations" accept that this data protection measure should not cover security services dealing with national security. It is noted that there can be extensive exchanges between the security agencies and the police. Tony Bunyan, Statewatch editor, comments: *"If the security agencies are not to be covered by this Framework Decision on data protection are they to be subject to another measure, or are they above the law?"*
The draft, which has been "carefully crafted", also excludes law enforcement agencies when undertaking "intelligence activities in the field of national security" from the scope of the draft Framework Decision.
Another contentious provision is a watered down provision on "processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade-union membership and the processing of data concerning health or sex life". As the Council document notes the Commission proposal called for a strict "regime" (based on the Council of Europe Convention no 108) and laid down: "a general prohibition of the processing of this type of data." The Council's draft - mindful that their position will set a "standard": "which is likely be referred to in other contexts as well (e.g. PNR negotiations with third countries)" proposes a lower "standard": "when this is strictly necessary and when the domestic law provides adequate safeguards."
81. SKIM 2000 project, Dutch police, sexual abuse, exploration amongst juvenile victims. (Aangifte van seksueel misbruik, Een verkenning onder jeugdige slachtoffers)
mr. S. Meuwese Justitiële verkenningen, jrg. 26, nr. 6, 2000, p. 79.
82 Directive Child pornography (De aanwijzing Kinderpornografie) 30 July 2007 (Stcrt. 2007, 162): (realistische, niet van echt te onderscheiden afbeeldingen)

It is the choice of democratic states to decide how to protect the fundamental values of the citizen and what values prevail. If a choice has to be made this at least has to be a democratic choice.

Tony Bunyan, Statewatch editor, comments:[83]

> This is going to be a momentous decision affecting existing national laws on data protection, and the exchange of data within the EU and around the globe. It is also going to the foundation of the right of data protection in a host of planned and future EU measures, including the new Schengen Information System (SIS II).
> The Commission draft proposal is being substantially re-written by the Council's Multidisciplinary Group on Organised Crime including removing the rights of data subjects and obstacles to the passing of data to third countries outside the EU.
> Until the Council finishes its so-called "second reading" the final text will not been known - when they are intending to simply "nod" it through. If it does so without the opportunity for national and European parliaments and civil society to express their views it will utterly lack legitimacy.

Criminal law is the most intrusive law that is agreed upon in society and must be handled with the utmost scrutiny by authorities. Treatment of the privacy of data subjects should be proportionate to the seriousness of the crime but also to the phase of the process where these data are handled taking in consideration the purpose of the tasks in a democratic society.

[83] http://www.statewatch.org/