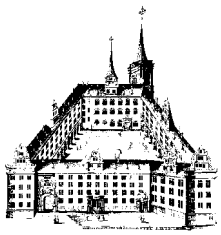


Legal Aspects of Computer-Related Crime in the Information Society – COMCRIME-Study –

prepared for the European Commission
by
Prof. Dr. Ulrich Sieber
University of Würzburg

Version 1.0 of 1st January 1998

Disclaimer

The views expressed in the present study are the author's and do not necessarily correspond to the views of the European Commission.

Legal Notice

Neither the Commission of the European Community nor any person acting on its behalf is responsible for the use which might be made of the following information.

Executive Summary

This study is based on a contract between the European Commission (DG XIII) and the University of Würzburg. Its aim is to provide the European Commission with up-to-date information on the legal issues of computer-related crime, especially with respect to substantive criminal law, procedural criminal law as well as the suggestion of alternative solutions. The contract also includes the establishment of a database with the relevant national computer crime statutes of substantive criminal law. The following executive summary focuses on some of the main findings of the study.

1. Vulnerability of the Information Society

The *vulnerability of today's information society* in view of computer crime is still not sufficiently realised: Businesses, administrations and society depend to a high degree on the efficiency and security of modern information technology. In the business community, for example, most of the monetary transactions are administered by computers in form of deposit money. Electronic commerce depends on safe systems for money transactions in computer networks. A company's entire production frequently depends on the functioning of its data-processing system. Many businesses store their most valuable company secrets electronically. Marine, air, and space control systems, as well as medical supervision rely to a great extent on modern computer systems. Computers and the Internet also play an increasing role in the education and leisure of minors. International computer networks are the nerves of the economy, the public sector and society. The security of these computer and communication systems and their protection against computer crime is therefore of essential importance.

In the course of this development *computer crime* has developed into a major threat of today's information society. The spreading of computer technology into almost all areas of life as well as the interconnection of computers by international computer networks has made computer crime more diverse, more dangerous, and internationally present. An analysis of relevant "criminogenic" factors shows that modern computer and communication networks have specific characteristics which are highly useful for perpetrators but which imply difficulties for potential victims and for law enforcement (such as complex security questions, multiple hardware and software systems, inexperience of many users, anonymity, encryption

and international mobility). Groups active in organised crime, professional business espionage and secret services around the world are already exploiting these new features of computer crime. However, many governments, businesses and private users are not aware of the attacks that happen or could happen to them in the DP-area. Thus, governmental agencies, the industry and private users should be made aware that protection against computer attacks is of great significance. They should be informed about the main threats of computer crime and the responses thereto.

The present study first systematises the necessary basic information on the vulnerability of the information society by computer crime. As a prerequisite for identifying the relevant problems and for finding solutions, the report gives an *empirical analysis* of the relevant problems. Using actual case-studies, it describes especially infringements of privacy, economic crimes, violations of intellectual property and dissemination of illegal contents. The analysis shows that at present, the focus of computer crime lies in the field of economic crimes, such as computer fraud, hacking, computer espionage and theft of intellectual property. However, the use of modern computer and communication technology in traditional fields of organised crime (such as drug and weapons dealing) is gaining importance. Illegal and harmful contents in computer networks are increasingly worrying the public, too, thus creating a serious threat for the acceptance of the new media.

2. Present Legal Situation

According to the contract between the European Commission and the University of Würzburg, the main aim of the study is to analyse the legal issues of computer crime. This analysis shows:

On the national level, comprehensive and international answers to the new challenges of computer crime are still missing. In most countries, reactions to computer crime focus too much on national (especially criminal) law, neglecting alternative protective measures. However, even in the legal field, there are considerable deficits. Despite successful efforts of international and supranational organisations, the various national laws show remarkable differences, uncertainties or loopholes especially with respect to the criminal law provision on infringements of privacy, hacking, trade secret protection and illegal contents. Considerable differences and uncertainties also exist with respect to the responsibility of Internet providers, coercive powers of prosecuting agencies (especially with respect to encrypted data and investigations in international computer networks) as well as the range of jurisdiction in criminal matters.

On the international and supranational levels, various organisations have co-ordinated or harmonised activities against computer crime. Besides the European Union (with a number of activities both under the first and the third pillar), these are especially the Council of Europe, the P8, the OECD, Interpol and the United Nations. These international and supranational efforts have increased considerably in recent years: Whereas in the 1970s and 1980s, there was a lack of international activities, today there is a lack of co-ordination among the various organisations, which risk starting redundant programs. Moreover, many of the present international and supranational answers are too vague and concentrate too much on legal issues.

3. Necessary Future Solutions

As a prerequisite for finding future strategies to fight computer crime, the report analyses the basic changes of the international risk and information society as the driving forces behind computer crime. Based on this analysis, the study stresses three main requirements for future strategies: Future solutions must be international, comprehensive and – especially in the legal area – devoted to the specifics of information:

- Future measures against computer crime must be *international* since different national strategies with the aim of preventing computer crime would create "data havens" or "computer crime havens" which, in turn, would lead to market restrictions and national barriers to the free flow of information and Europe-wide services. Above all, national solutions and restrictions for the free flow of information would be doomed to failure since the amount of data transferred in international computer networks makes the control of their content neither possible nor socially desirable.
- Future measures against computer crime should aim at *comprehensive solutions* including non-legal measures. This is especially important since the new threats of today's risk society require broader concepts of prevention that go beyond purely criminal interdictions. Non-legal remedies – such as technology, education and industry self regulation – can often be much more effective than tightening criminal law provisions which – especially in the field of procedural law – can also infringe civil liberties.
- All solutions must be *specific solutions* considering the differences between tangible and intangible property. This is especially important for legal remedies: Information is a new and distinct value which cannot be protected in analogy to corporeal objects. In the legal field, this requires a new doctrine of information law dealing especially with the protection of the author and holder of information, the protection of the person

concerned by information, the protection of society against illegal and harmful information as well as access-to-information rights.

Based on the changes of the international risk and information society and these three requirements, the report suggests a comprehensive set of measures to fight computer crime especially by *four main remedies: technology, education, industry and the law.* These four remedies are first illustrated in general. They are then specified with respect to concrete recommendations for the European Union.

4. Specific Recommendations for the European Union

The European Community has already enacted directives with precise requirements for the harmonisation of the (non-criminal) provisions of data protection law and intellectual property protection. Deficits of clearly defined European solutions exist especially with respect to non-legal measures as well as with respect to economic criminal law, illegal and harmful contents, criminal procedural law, security law as well as the sanctions in the field of data protection law. This could be changed by the following actions:

In the non-legal sector, priority actions of the European Union could especially support

- improved intelligence especially with respect to an analysis of the links of high tech crime and organised crime
- higher awareness and education (since most cases of computer crime are caused by a lack of awareness of users)
- sophisticated technological measures and new research projects in computer security (especially with respect to electronic commerce and safe money transactions)
- a network of contact points for illegal contents (to support an adequate legal framework)
- international industry codes of conduct (especially with respect to illegal contents, illegal activities and protocols for international police co-operation)
- development of trace-back procedures (especially by bringing together lawyers, prosecutors and industry to develop, implement and use additions to the TCP/IP protocols supporting such procedures), as well as continued co-ordination of the various international activities in wiretapping issues.

Legal measures under the first pillar can be based on Article 100a of the Treaty on the European Union. They could primarily focus on

- the elaboration of a directive on the general (civil and criminal) *responsibility* of access and Internet service providers (which should be elaborated before more national laws will enact such regulations)
- the consideration of a directive which could define legal, illegal and harmful *contents* in computer networks, which could not only require Member States to create effective sanctions against these illegal and harmful contents but also prohibit Member States to restrict international data flow with respect to illegal and harmful contents not listed in the directive
- the inclusion of a list of illegal *acts* to be prohibited and covered by adequate sanctions of national law in a future directive (e.g. on electronic commerce) in order to guarantee security and consumer protection in European computer networks
- improved information on the legal situation in the Member States (e.g., by amending and updating the corpus iuris database on computer crime statutes).

Legal measures under the third pillar could concentrate on joint actions (or, under the Amsterdam Treaty, framework decisions), in co-operation with the Council of Europe and the P8 group. However, the EU should constantly look for a closer co-operation within the European Union than is possible within the framework of the other international organisations. The joint actions or framework decisions could be adopted with respect to

- defining minimum rules for fighting international computer crime by criminal law
- recommending adequate coercive powers with respect to the investigation of computer crime in international computer networks (balancing the requirements for effective prosecution and for human rights of suspects and witnesses)
- fostering transborder investigations in international computer networks (especially transborder "online" investigations and freezing operations)
- defining the range of national jurisdictions in international computer networks (especially solving conflicts of jurisdiction arising in international computer networks, e.g., with respect to illegal contents which could fall under a multitude of jurisdictions)
- creating a set of common rules for a harmonised record-keeping in police and judicial statistics as well as for statistical analysis in specific fields of (especially computer) crime.

In order to *avoid redundant work by various international and supranational organisations*, the European Commission could start its work by

- organising a joint conference or a workshop of the major players in the fight against computer crime (European Union, Council of Europe, P8, OECD, Interpol and United Nations) with the aim of bringing together and co-ordinating the work of these organisations. A decision should be taken in how far the EU should develop the proposals mentioned above on its own or whether it should refer to proposals of other international bodies (the analysis of this report being the stating point for this co-ordination effort).

5. Corpus Iuris Database on Computer Crime Statutes

In order to improve the information on the various national laws, the present study provides a legal database with national computer crime statutes which were collected for this study. The data base can be searched systematically or via full text retrieval. The report recommends extending and updating this database and making it available in the World Wide Web.

This could be the starting point for an initiative to provide more information on the legal answers to computer crime. Such an initiative should not be limited to industrialised nations, but should also include developing countries since computer crime havens in developing countries could be as detrimental as computer crime havens in the Member States of the European Union, the P8 or the OECD.

Overview

Volume 1:
General Report by Prof. Dr. Ulrich Sieber

Volume 2:
Annexes: Special Law and Country Reports

Table of Contents

Volume 1:

General Report by Prof. Dr. Ulrich Sieber

Preface

This study originates from the public tender of the European Commission on computer-related crime which was published in the Official Journal C 206/12 of 11 August 1995. The tender was awarded to the University of Würzburg which received the respective contract on the 11 October 1996.

According to the contract between the European Commission and the University of Würzburg, the aim of the study was "to provide the European Commission with up-to-date information on the legal issues concerning computer-related crime, establishing the necessary links with the development of the information society." Tasks to be undertaken in this study included an in-depth analysis of the substantive law aspects describing the situation in the European Union, the United States of America and Japan, a description of procedural law aspects, suggesting alternative legal solutions, as well as supply of a database with retrieval software containing a systematic collection of national computer crime statutes in the field of substantive law.

The study is based on former reports which the author has written for the OECD, the Council of Europe, the UN and the AIDP. In order to gather additional material, the University of Würzburg co-operated with various institutions and research facilities: Based on a detailed questionnaire, it was tried to obtain country reports from all legal orders to be covered in the report. Comprehensive country reports were produced by Dr. *Gabriele Schmölzer* for Austria; Prof. *Jos Dumortier* and Mr. *Patrick Van Eecke* for Belgium; Mr. *Donald K. Piragoff*, B.A., LL.M., for Canada; Mr. *Antti Pihlajamäki*, LL.Lic., for Finland; Dr. *Manfred Möhrenschlager*, M.C.L., for Germany; Dr. *Irini Vassilaki* for Greece; Prof. *Atsushi Yamaguchi* for Japan; Mr. *Marc Jaeger* for Luxembourg; *J.P.G.M. Verbeek* and Prof. Dr. *Henrik W.K. Kaspersen* for the Netherlands; Prof. Dr. *José de Faria Costa* and Mrs. *Helena Moniz* for Portugal; Dr. *María Luz Gutiérrez Francés* for Spain; Prof. Dr. *Nils Jareborg* for Sweden; Prof. Dr. *Martin Wasik* for the United Kingdom and Prof. *Edward M. Wise* for the United States of America. Furthermore, the research on the procedural law aspects was supported by a report of Professor *Henrik Kaspersen* of the Vrije Universiteit Amsterdam, who had been the chairman of the Council of Europe's expert committee on procedural law aspects of computer-related crime.

Additional specific country reports which include the new issues on pornography and hate speech on the Internet have been prepared under the supervision of Prof. Dr. *Albin Eser* and Dr. *Karin Cornils* by collaborators of the Max Planck Institute for Foreign and International Criminal Law in Freiburg, especially by Mr. *Holger Barth* for France and Luxembourg; Mrs. *Frauke Eickhoff-Pritzl* for Belgium and the Netherlands; Mrs. *Susanne Hein* for Italy; Mrs. *Hofmann* for Spain; Mr. *Fred Münch* for Switzerland and other collaborators for Sweden, Denmark, Finland, Ireland and the United Kingdom. Further specific material and help was provided by Attorneys at Law *André R. Bertrand* et Associés (Paris/France), Attorney at Law Dr. *Cristina Busch* (Barcelona/Spain), Mr. Ph. D. *Derksen* of the Scientific Service of the German Bundestag (Bonn/Germany), Mr. *Phillippe Gérard* (Namur/Belgium), Mrs. *Eanna Hickley* (Dublin/Ireland), Mr. *Pablo Mathonnet* (Paris/France), Mrs. *Betty-Ellen Shave* from the US Department of Justice (Washington D.C./USA), Mr. *Matti Tenhunen* (Vantaa/Finland), Attorneys at Law Dr. *Ursula Widmer* & Partner (Bern/Switzerland). Further support has been provided by Mr. *Ekkehart Kappler,* computer expert of the German Bundeskriminalamt (Wiesbaden/Germany) and Chairman of the Interpol Working Group on Information Technology and Crime.

Valuable help and information has also been given by Mr. *George Papapavlou* and Dr. *Günther Willms* of the European Commission who have been responsible for the execution of the contract on the present study on behalf of the European Commission.

Additional research on available literature on paper, databases and on the Internet was done by members of my staff at the University of Würzburg, especially by Mr. *Stephan Bleisteiner*, LL.M., Mr. *Jan Hendrik Dopheide*, Mr. *Bernhard Günther*, Mr. *Stefan Felixberger*, Mr. *Jörg Knupfer*, and Mr. *Hans Kudlich* all of whom also assisted in the compilation of the material. The relevant law texts were collected in a database which was programmed by my collaborator Mr. *Daniel Stricharz* and organised and entered by Mr. *Andreas Hornung*, Ms. *Angelika Laitenberger*, Ms. *Anja Schleyer*, Ms. *Annette Volk* and Ms. *Susanne Walz*. The typing, proof-reading and the layout of the report and of the annexed country reports was done by Ms. *Margit Hohmann,* Mr. *Gundolf Schweppe,* Mr. *Tobias Sedlmeier* and Ms. *Nicole Selzam*.

I would like to thank all of these persons for their most valuable support!

Würzburg, 1st January 1998

Ulrich Sieber

I. Introduction to the Topic

A. The Concept of Computer Crime

1. Historical Development and Definition

The history of "computer crime" dates back to the 1960s when first articles on cases of so-called "computer crime" or "computer-related crime"[1] were published in the public press and in scientific literature. These cases primarily included computer manipulation, computer sabotage, computer espionage and the illegal use of computer systems. However, due to the fact that most reports were based on newspaper clippings,[2] it was controversially discussed whether or not this new phenomenon of computer crime had any plausible reasons.[3]

It was not before the mid-1970s that the first empirical computer crime studies applying scientific criminological research methods were conducted.[4] These studies brought to light a limited number of verified computer crime cases, but at the same time suggested a high estimated number of undetected or unreported cases of computer crimes. They also investigated some spectacular computer crime cases such as the American Equity

1 Both terms are used synonymously here.

2 See, e.g., for the Federal Republic of Germany, *von zur Mühlen*, Computer-Kriminalität – Gefahren und Abwehr, 1973; for the United States of America, *Parker/Nycum/Oüra*, Computer Abuse, 1973.

3 See for the Federal Republic of Germany, *Betzl*, Computerkriminalität – Dichtung und Wahrheit, (1972) Datenverarbeitung in Steuer, Wirtschaft und Recht, p. 317; for the United States of America compare the later published analysis of *Taber*, A survey of computer crime studies, (1980) Computer and Law Journal, pp. 275 et seq.

4 See, e.g., for the Federal Republic of Germany, *Sieber*, Computerkriminalität und Strafrecht, 1st ed. 1977, 2nd ed. 1980; for Sweden, *Solarz*, Computer Technology and Computer Crime, Report No. 8 of the Research and Development Division, National Council of Crime Prevention, 1981. For the European Communities, see European Communities' Information Technology Task Force, The Vulnerability of the Information-Conscious Society, 1984.

Funding case,[5] the German Herstatt case,[6] or the Swedish Volvo manipulations.[7]

The public and scientific view of computer crime radically changed in the 1980s, when the press published astonishing cases about hacking, viruses and worms.[8] Furthermore, a broad wave of program piracy, cash dispenser manipulation and telecommunication abuses revealed to a broad public the vulnerability of an information society and such also the need for a new strategy of DP-security and crime control. It also appeared that computer crime was no longer limited to economic crime, but included attacks against all kinds of interests, such as the manipulation of a hospital computer or computer-related infringements of privacy, which were originally discussed separately from "computer crime". Thus, it became clear that the notion of computer crime had to be established as a broad concept, which, later in the 1990s, could integrate the distribution of illegal contents on the Internet as well as include the use of computers and communication systems by groups of organised crime.

As a consequence, already in 1983 a group of experts of the OECD defined the term "computer crime" (or "computer-related crime") as any illegal, unethical, or unauthorised behaviour involving automatic data-processing and/or transmission of data.[9] Later studies went even further in

---

5 The Equity Funding Fraud involved manipulations of 56,000 insurance claims with a sales value of at least US$ 30 million. In 1973, it resulted in compensation claims of US$ 1 to 2 billion. See *Sobbel/Dallos*, The Impossible Dream, 1975; *Loeffler*, Report of the Trusty of Equity Funding Corporation of America, 1974.

6 The Herstatt case concerned speculative foreign exchange transactions totalling several billion dollars which were not recorded in the Herstatt bank's account files. The bankruptcy of the bank in 1974 caused losses to the bank's customers of about DM 1.2 billion. See *Sieber*, Computerkriminalität und Strafrecht, 2nd ed. 1980, pp. 61 et seq.

7 See *Solarz*, Computer Technology and the Transformation of Criminality, in: Strömholm/Hemström (eds.), Swedish National Reports to the XIIIth International Congress of Comparative Law, 1990, pp. 285 et seq. (at pp. 292 et seq.).

8 The danger of "hacking" became especially evident in 1989 when criminal proceedings in the Federal Republic of Germany identified German hackers who were using international data networks to gain access to information inside American, British, and other foreign computer systems in order to sell their findings to the former Soviet secret service KGB. For the details of the case, see *Ammann/Lehnhard/Meißner/Stahl*, Hacker für Moskau, 1989; *Hafner/Markoff*, Cyberpunk, 1991, pp. 139 et seq.; *Stoll*, The Cuckoo's Egg, 1989. Around the same time, the peril of viruses and worms became especially obvious when the "Internet-worm" created by an American student affected and closed down about 6,000 computer systems within the "Internet"-network in only a couple of days. For details see *Hafner/Markoff*, Cyberpunk, 1991, pp. 251 et seq.; *Weihrauch*, Der Morris-Wurm im Internet, (1988) Datenschutz-Berater, issue 12, pp. 1 et seq.

9 See *Sieber*, The International Handbook on Computer Crime, 1986, pp. 1 et seq.

developing broader concepts on "data and/or information crime".[10] The breadth of these definitions proved to be advantageous as it allowed the use of the same working hypothesis for all kinds of criminological, criminalistic, economic, preventive and legal studies. Nevertheless, this general definition did not prevent each of these studies from only dealing with the phenomena of computer crime which cause computer-specific problems in their own discipline.[11] The present study follows this definition and methodology: It is based on the broad concept of computer crime, as defined by the OECD. However, the legal part of the study will focus on computer-related criminal law creating computer-specific legal problems.

2. Statistical and Qualitative Development

a. Quantitative Aspects: Computer Crime Statistics

In order to evaluate the relevance of computer crime, criminological researches often referred to statistics concerning computer crime cases. Such general statistics on "computer crime" were in particular developed in the 1970s and 1980s, when the phenomena of computer crime revealed a homogeneous pattern which consisted predominantly of fraud, sabotage and espionage cases. These statistics were elaborated by criminologists, as well as by police authorities, and resulted in only small numbers of verified cases of computer crime.[12]

However, after the dramatic rise in program piracy, cash dispenser manipulations and hacking cases since the mid-1980s, such general

10 See, e.g., for the respective problems of definition *Bloom/Becker*, Spectacular Computer Crimes, 1990, pp. 69 et seq.; *Kaspersen*, Strafbaarstelling van computer mis-bruik, 1990, p. 342. For the general concept of "(criminal) information law" see *Sieber*, The International Emergence of Criminal Information Law, 1992, pp. 11 et seq.; *Sieber*, Informationsrecht und Recht der Informationstechnik, (1989) Neue Juristische Wochenschrift, pp. 2569 et seq.

11 It is clear that more specific definitions and a more detailed classification of the various phenomena of computer crime are dependent on the respective research aim. Consequently, technically oriented classifications (e.g. distinguishing between the computer as a tool or an object of crime) as well as sociological differentiations (e.g. distinguishing between insider and outsider offences) have only a limited value for legal analysis. Until now, combined legal and criminological distinctions based on the attacked interests proved to be most valuable for legal research since the criminal codes of most countries are structured in the same way. In consideration of this fact, the majority of traditional criminological and legal computer crime studies distinguish between computer-related economic crimes, computer-related infringements of privacy, and attacks on other legally protected interests.

12 For an overview on these statistics see *Sieber*, The International Handbook on Computer Crime, 1986, pp. 29 et seq.

statistics have lost their former relevance and were not continued in many countries. Today, only statistics that differentiate are significant, due to the variety of computer crime cases and the high number of specific phenomena. In some countries, these differentiated crime figures can be obtained from official crime statistics.

- E.g. in Germany, the police registered 32,128 cases of "computer crime" in 1996: 26,802 cases of cash-dispenser manipulations, 3,588 cases of computer fraud, 198 cases of forgery of computer data, 282 cases of alteration of data and computer sabotage and 933 cases of illegal obtainment of computer data (especially "hacking cases").[13]
- In the Netherlands, statistics were only kept until 1992.[14] From 1981 until 1992, about 1,400 cases became known. Nearly one third belonged to the technical support of criminal investigations. More than 10% were cases of hacking. Computer piracy reached 15% and computer viruses approximately 30%. During the reported time, the number of cases was constantly increasing.
- In Japan, only a few cases of computer crime are known to the police. Between 1971 and 1995 there were 14 cases of destruction of hardware, 12 cases of falsification or erasure of data, 7 cases of illegal use of hardware, 12 cases of theft of data and programs and 615 cases of falsification or erasure of data. In 1995, police learned a total of 168 new computer crimes; card crimes (which are not included in the statistics on computer crime in Japan) totalled 6,671.[15]

It is clear that these numbers of verifiable cases do not permit to draw any conclusions concerning the number of actual cases, since the number of undiscovered offences in computer crime is estimated to be considerably higher. This assumption is first and foremost based on the low proportion of computer offences which became known as a result of the specific difficulties of detection and proof in the DP-sector. Moreover, many of the revealed offences are subject to the internal disciplinary procedures of the concerned companies. This is based on the fact that most companies are afraid to cause any damage to the companies' reputation and to lose the investors', shareholders', and customers' confidence, or that they prefer to facilitate the compensation for the damage and therefore do not report the offences to the public. Furthermore, cases reported to the law enforcement

13 Polizeiliche Kriminalstatistik 1996, pp. 250 et seq.

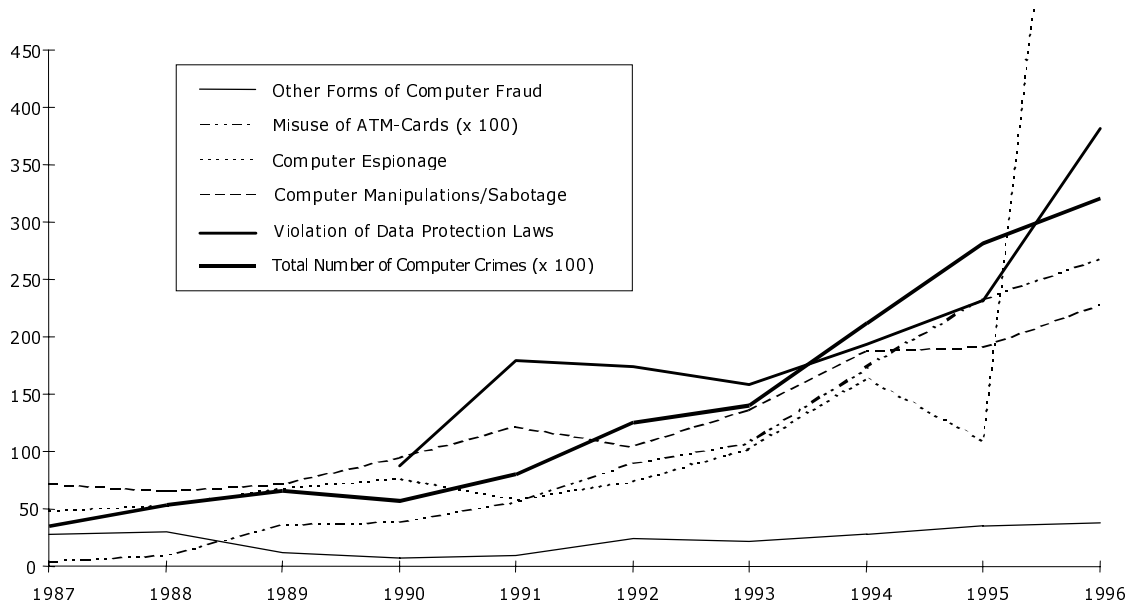
14 C.R.I. – Centrale Recherche Informatiedienst, Annual Report 1989-1991, Erahatie Pilotproject Computercriminaliteit, The Hague 1992.

15 See National Police Agency, White Paper on Police 1996 (Excerpt), 1996, pp. 68 et seq.

agencies are not always systematically prosecuted, since an effective treatment of these cases requires special knowledge as well as high expenditure in terms of time and 500money. In addition, in many areas it is a matter of chance whether reported cases of computer crime are discovered among cases of espionage, copyright infringements and other general criminal provisions, because the criminological term "computer crime" only partly appears in official legal statistics.

As a consequence, the absolute numbers indicated in differentiated and specialised statistics are only of limited value. However, if these statistics are conducted in a similar manner over the years, they can show trends in the development of specific computer crimes. Using the differentiated German police statistics in the fields of computer crime, this development is characterised by a significant rise of cases of illegal obtainment of computer data. The following table based on the German police statistics evidently shows a sharp rise of computer crime in recent years and is important evidence for the seriousness of the respective problems.

German Police Crime Statistics: Number of Computer Crimes Reported to the German Police



b. Qualitative Aspects: The Vulnerability of the Information Society

In recent years, the lack of exact figures on computer crime has become less important in evaluating the social relevance of computer crime. In an era where society is becoming more and more dependent on information technology, the importance of computer crime for the society is based not on quantitative, but rather on qualitative aspects. The analysis of these qualitative aspects shows the real threats and dangers of computer crime: In the business community, the majority of monetary transactions is administered by computers in the form of deposit money. In the future, electronic commerce will depend on safe money transactions. Balance sheets are prepared with computer support. A company's entire production is frequently dependent on the smooth functioning of its data processing system. Furthermore, many companies store their most important business secrets electronically. Modern administration relies on computer technology and databases in a similar way. Marine, air and space control systems, medical supervision as well as defence systems also depend to a great extent on computer technology. International computer networks are becoming the nerves of the economy, the public sector and society. Consequently, there can be no doubt that the security of information technology and the prevention of computer crime is of decisive significance for today's information society.

3. The Need for Specified Risk Analyses

One of the main dangers of computer crime is caused by the fact that many private users do not know the threats that they are actually or potentially exposed to. Similarly, many governmental agencies, law makers and politicians are not aware of the risks and vulnerabilities of the computerised information society. What is necessary, therefore, is a differentiated risk analysis of computer crime cases.

According to the underlying contract, the present study does not aim at an empirical research of computer crime but primarily at an analysis of computer-related law. However, with respect to the above-mentioned developments, the study will start with a short overview on the relevant risks and vulnerabilities (infra chapter II). This basic analysis of the different forms of computer crime in the information society will then serve as a valuable basis for the analysis or computer-related law problems and for the development of a general strategy of protection against computer crime.

B. The Concept of Computer-Related Criminal Law

1. Driving Forces

The concept of *computer-related criminal law* has undergone similar changes as the concept of *computer-related crime:* Many of the above-mentioned new forms of crime led to new computer-specific legal questions and law reform, thus broadening the concept of computer-specific criminal law and legislation. Especially since the 1970s, there has been a growing number of law reform projects in many countries.

The reason for this adaptation of the law to new forms of crime was not only based on technical changes, but mainly on fundamental changes of paradigms: Until the middle of the 20th century, the criminal codes of all countries have predominantly protected tangible objects.[16] However, towards the end of the 20th century, the emerging information society has led to an increased importance of incorporeal values and information. These new values could not be protected in analogy to corporeal objects, but required new legal provisions. Thus, the field of computer-related criminal law soon became a complex field of many different new legal questions.

2. The Main Waves of Computer Crime Legislation

Despite the multitude of new computer-specific legal questions, the emergence of computer-related criminal law (or criminal information law) can be systematised and traced back to six main waves of computer crime legislations, which today still characterise the six main fields of criminal information law and therefore will be the basis of the legal analysis of the present study.

a. Protection of Privacy

The first wave of law reform in most western legal systems emerged in the field of privacy protection in the 1970s and 1980s. This legislation was a reaction to new challenges of privacy caused by expanded possibilities for

16 The protection of information and other intangibles existed, but did not play a dominant role until the middle of the 20th century. See, e.g., the criminal law provisions on state, trade and professional secrets, on patent and copyright protection and on forgery.

collecting, storing and transmitting data by new technologies. "Data protection laws" were enacted and have been constantly revised and updated, protecting the citizens' right of privacy with administrative, civil, and penal regulations in 1973 in Sweden, 1974 in the United States of America, 1977 in the Federal Republic of Germany, 1978 in Austria, Denmark, France and Norway, 1979 and 1982 in Luxembourg, 1981 in Iceland and Israel, 1982 in Australia and Canada, 1984 in the United Kingdom, 1987 in Finland, 1988 in Ireland, Japan and the Netherlands, 1991 in Portugal, 1992 in Belgium, Spain and Switzerland, 1995 in Spain, and 1997 in Italy and Greece.[17] Additional data protection laws can be found

17 See, for *Australia*, the Freedom of Information Act of 9 March 1982, as amended and the Privacy Act 1988; for *Austria*, the Federal Data Protection Act of 18 October 1978, amended by laws Nos. 370 of 1986, 605 of 1987 and 632 of 1994; for *Canada*, the Access to Information Act and the Privacy Act of 28 June 1982; for *Belgium*, the law for the Protection of the Private Life with Respect to the Treatment of Personal Data of 8 December 1992; for *Denmark*, the Private Registers Act of 8 June 1978 (Act No. 293), amended on 1 April 1988 and the Public Authorities' Registers Act of 8 June 1978 (Act No. 293), amended on 1 April 1988; for *Finland*, the Personal Data File Act No. 471 of 30 April 1987, Personal Registers Act of 4 February 1987 and chapter 38 of the Penal Code (as amended 1995); for *France*, the Act on Data Processing, Data Files and Individual Liberties (Act No. 78-17) of 6 January 1978, amended on 11 March 1988; for *Germany*, the Data Protection Act of 20 December 1990 (succeeding the Data Protection Act of 27 January 1977); for *Greece*, Data Protection Act (law 2472/1997), passed in April 1997 by the Greek Parliament; for *Iceland*, the Act Concerning the Systematic Recording of Personal Data (Act No. 39/1985) of 25 May 1981; for *Israel*, the Protection of Privacy Law (Act No. 5741/1981) of 23 February 1981, amended in 1985; for *Ireland*, the Data Protection Act (Act No. 25/1988) of 6 July 1988; for *Italy*, Law No. 675 of 31 December 1996, published in the Gazetta Ufficiale 8 January 1997; for *Japan*, the Personal Information Protection Act No. 95 of 16 December 1988; for *Luxembourg*, The Act Organising the Identification on Physical and Legal Persons by Number of 31 March 1979, the Act Regulating the Use of Nominal Data in Electronic Data Processing of 31 March 1979 and the Act concerning the Protection of Privacy of 11 August 1982; for *the Netherlands*, the Law on the Protection of Privacy in Connection with Personal Registration of 28 December 1988; for *New Zealand*, the Privacy Act 1993, amended by the Privacy Amendment Act 1993 and the Privacy Amendment Act 1994; for *Norway*, the Law on Personal Data Registers of 9 June 1978 (Act No. 48) amended by Law No. 55 of 12 June 1987, Law No. 66 of 20 July 1991 and Law No. 78 of 11 June 1993; for *Portugal*, Law 10/91 of 29 April 1991 on the Protection of Personal Data with Respect to Informatics, amended by Law 28/94 of 29 August 1994; for *Spain*, Art. 18 para. 4 of the Constitution and Law 5/1992 for the Regulation of the Automated Processing of Personal Data (LORTAD) of 29 October 1992, and Article 197 Criminal Code (Law No. 10/1995 of 23 November 1995); for *Sweden*, chapter 2 Article 3 para. 2 Instrument of Government (i.e., Constitution) as amended 1988; the Data Protection Act of 11 May 1973 (Law No. 289), amended 1979, 1982, 1986, 1990 and 1992); for *Switzerland*, Federal Data Protection Act of 19 June 1992; for the *United Kingdom*, the Data Protection Act of 12 July 1984; for the *United States of America*, the Privacy Act 1974 (5 U.S.C. § 552a) and the Electronic Communications Privacy Act 1986 (codified at 18 U.S.C. §§ 1367, 2232, 2510-2522, 2702-2711, 3117, 3121-3127). For detailed information on these reform laws cf. the references in Sieber (ed.), Information Technology Crime, 1994, in particular on Belgium *Spreutels* (p. 63), on Canada *Piragoff* (p. 120, fn. 127), on Finland *Pihlajamäki* (pp. 157, 159, 165), on France *Francillon* (pp. 179 et seq.), on UK *Wasik* (p. 499), on Hungary *Kertész/Pusztai* (pp. 252 et seq.), on Israel *Lederman/Shapira* (p. 264, fn. 6), on Japan

in many federalistic jurisdictions (e.g. Canada, the Federal Republic of Germany, Switzerland, or the United States of America) as well as in many "sectorial" laws regulating privacy protection in specific areas which today become increasingly important (e.g., in the area of telecommunication, police data or online services). In Brazil, the Netherlands, Portugal and Spain, privacy protection even brought about constitutional amendments.[18]

b. Economic Criminal Law

The second main wave of reform laws involved the repression of computer-related economic crimes at the beginning of the 1980s. This legislation became necessary as the relevant traditional criminal provisions exclusively protected physical, tangible and visible objects against traditional crimes. However, new forms of computer-related economic crime not only violate traditional objects in the form of new media (such as deposit money stored in computer records), but also involve intangible objects (such as computer programs or use of DP-facilities) or new methods of commission (e.g. manipulating a computer instead of cheating a person). Instead of stretching the wording of already existing provisions (which would contradict the principles of legality and the prohibition of analogy *in malam partem* in criminal law), many countries enacted new laws fighting computer-related economic crime (including illegal access to computer systems). Laws against computer-related economic crime were enacted since 1978 in the United States of America (in state legislation) and in Italy, since 1979 in Australia (state law), 1981 in the United Kingdom, 1984 in the United States of America (federal level), 1985 in Canada and Denmark, 1986 in the Federal Republic of Germany and in Sweden, 1987 in Austria, Japan and Norway, 1988 in France and Greece, 1990 in Finland and the United Kingdom, 1992 in the Netherlands, 1993 in Luxembourg, 1994 in Switzerland, 1995 in Spain

Yamaguchi (p. 317), on Luxembourg *Jaeger* (p. 327, fn. 11), on the Netherlands *Kaspersen* (p. 358, fn. 49), on Portugal *de Faria Costa* (p. 396, fn. 24), for the regulations in detail pp. 396 et seq.), on Spain *Gutiérrez Francés* (pp. 431 et seq., 439), on Sweden *Jareborg* (p. 443), on Switzerland *Roth* (p. 471, fn. 59, for the regulations in detail pp. 471 et seq.), on the USA *Wise* (pp. 518, fn. 49, 525 et seq.). For a comparative overview see *Nugter*, Transborder Flow of Personal Data within the EC, 1990.

18 See, e.g., for Portugal, Article 35 of the Constitution; for Spain, Article 18.4 of the Constitution; for the Netherlands, Article 10 of the Constitution; for Brazil, Article 5 (0) X of the Constitution. For an overview on the various privacy acts and bills see *Flaherty*, Protecting Privacy in Surveillance Societies, 1989; *de Houwer/van Brabant*, The Transborder Flow of Personal Data, 1989 (edited by the International Criminal Law Center Bruxelles), pp. 51 et seq.; *Nugter*, Transborder Flow of Personal Data within the EC, 1990; *Sieber*, The International Handbook on Computer Crime, 1986, pp. 96 et seq.

and again in Finland, and 1997 in Malaysia.[19] In countries such as Denmark, the Federal Republic of Germany or Finland, the respective laws also included new provisions for trade secret protection.[20] While some countries operate under the legal provisions enacted since the early 1980s, other countries such as, e.g., Canada are currently amending these provisions again to reflect new challenges to computer-related criminal law posed by the fast developing computer technology.[21]

c. Protection of Intellectual Property

In the course of the 1980s a third series of law amendments improved the protection of intellectual property in the field of computer technology.

---

19 See, for Austria, the Criminal Code Amendment Act of 1987 (Bundesgesetzblatt 1987/605); for Australia, Section 408e of the Queensland Criminal Code as amended in 1979, Sections 222, 276 of the Northern Territory Criminal Code as amended in 1983, Section 115 of the New South Wales Crimes Act 1900 in its application to the Australian Capital Territory, as amended in 1985, the Crimes (Computers) Act No. 36 of 1988 of Victoria, as well as additional legislation passed in the Australian Capital Territory, the Commonwealth, New South Wales, the Northern Territory, South Australia and Victoria; for Canada, The Criminal Law Amendment Act 1985 (S.C. 1985, c. 19); for Denmark, the Penal Code Amendment Act of 6 June 1985 on Data Criminality; for Germany, the Second Law for the Suppression of Economic Crime of 15 May 1986 (Bundesgesetzblatt I, 1986, p. 721); for Finland, the Laws Amending the Criminal Code No. 769/1990 of 24 August 1990 (first phase of the total reform of the Criminal Code), and No. 578/1995 of 28 April 1995 (second phase of the total reform of the Criminal Code); for France, the Law on Infringements in the Field of Informatics of 5 January 1988; for Greece, Law No. 1805/88 of 30 August 1988; for Italy the Amendment of 1978 to Section 420 Penal Code (concerning attacks to public utility plants and research or data processing facilities); for Luxembourg, Law of 15 July 1993 Aiming to Reinforce the Fight Against Economic Crime and Computer Fraud; for Malaysia, Computer Crime Law of 1997; for the Netherlands, Dutch Computer Crime Act of 23 December 1992, as amended in 1994 and 1995; for Japan, the Penal Code Amendment Act of 1987; for Norway, the Criminal Code Amendment Act of 12 June 1987; for Spain, Criminal Code 1995 (Law No. 10/1995 of 23 November 1995), especially Articles 248.2, 256, 264.2, 278 et seq.; for Sweden, Section 21 Data Protection Act of 4 April 1973, and the Criminal Code Amendment Act of July 1986 (Law No. 123); for Switzerland, 1994 Revision of Property Crime Provisions; for the United Kingdom, the Forgery and Counterfeiting Act of 1981, and the Computer Misuse Act 1990 of 29 June 1990, draft for a new Section 15a Theft Act 1968; for the United States of America, the Credit Card Fraud Act of 1984 (Publ. L. 98-473) and the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 and the Computer Fraud and Abuse Act of 1986 (both codified as amended at 18 U.S.C. §§ 1029-1030) as well as State legislation in every state but Vermont. For a comparative analysis of the various laws see *Sieber*, The International Handbook on Computer Crime, 1986, pp. 42 et seq.

20 See also the references infra chapter III.B.3.

21 See, e.g., for Canada, The Criminal Law Improvement Act, 1997 (Bill C-17, the proposed Criminal Law Improvement Act, 1996, 2nd Session, 35th Parliament, 45 Elizabeth II, 1996) which will inter alia prohibit the unauthorised use and trafficking of computer passwords and the possession of devices useful for committing computer offences (new Sections 342.1 (1) (d) and 342.2).

Having excluded computer programs from patent protection in the 1970s,[22] reform laws which explicitly provided *copyright protection for computer programs* were enacted in 1972 in the Philippines, 1980 in the United States of America, 1983 in Hungary, 1984 in Australia, India and Mexico, 1985 in Chile, the Federal Republic of Germany, France, Japan, and the United Kingdom, 1987 in Brazil, Canada and Spain, 1988 in Canada, Denmark and Israel, 1989 in Sweden, 1990 in Norway, 1991 in Finland, 1993 in Austria, and 1995 in Luxembourg.[23] The development concerning the *legal protection of topographies* was different. A 1986 EC Directive on the legal protection of topographies of semiconductor products[24] forced the Member States of the

22 In Europe, rules and methods for performing mental acts are not regarded as patentable inventions. Due to this principle, Article 52 (2) and (3) of the European Patent Convention (EPC, Munich, 1973) excludes patentability of computer programs as such. In most European countries this limitation of patentability can be found in the national patent legislations. See, for example, for Austria, Section 1 (2) No. 3 Patent Law, amended 8 June 1984 (Bundesgesetzblatt 1984/234); for France, Sections 6 and 11 Patent Law No. 68-1 of 2 January 1968, modified by Law No. 78-742 of 13 July 1978 and Law No. 84-500 of 27 June 1984; for Germany, Section 1 (2) No. 3 and (3) Patent Law of 5 June 1936, amended on 16 December 1980; for Italy, Section 12 Patent Law No. 1127 of 29 January 1939, modified by Law No. 338 of 22 June 1979; for the United Kingdom, Section I (2) (c) of the Patents Act 1977.

23 See, for Australia, the Copyright Amendment Act 1984 on Informatics; for Austria, Copyright Amendment Act 1993 (Bundesgesetzblatt 1993/93) as amended in Bundesgesetzblatt 1996/151; for Brazil, Law No. 7.646 of 18 December 1987; for Canada the Copyright Amendment Act 1988; for Chile, the Law on Intellectual Property of 7 October 1985; for Denmark, Law No. 153 of 14 January 1988; for Germany, the Copyright Amendment Act of 24 June 1985 (Bundesgesetzblatt I, 1985, p. 1137) and further amendments in Second Act to Amend the Copyright Act of 9 June 1993 (Bundesgesetzblatt I, 1993, p. 910); for Finland, the Copyright Amendment Acts No. 34/1991 of 11 January 1991, No. 418/1993 of 7 May 1993 and No. 446/1995 of 24 March 1995; for France, Law No. 85-660 of 3 July 1985 (loi relative aux droits d'auteur et aux droits des artistes-interprètes, etc.); for Hungary, Decree No. 15 of the Minister of Culture of 12 July 1983; for India, the Copyright Amendment Act No. XIX of 1984; for Israel, The Copyright Ordinance 1911 as amended in 1988; for Japan, the Copyright Amendment Act of 7 June 1985; for Luxembourg, the Act of 24 April 1995 amending the Copyright Act of 29 March 1972; for Mexico, the Copyright Amendment Act No. 114 of 8 October 1984; for Norway, the Copyright Amendment Act of 15 June 1990; for the Philippines, the Presidential Decree No. 49 of 14 November 1972; for Spain, Law No. 22/1987 on Intellectual Property of 11 November 1987, latest version passed by R.D. 1/1996 on 12 April 1996; for Sweden, the Copyright Amendment Act of 1989 (effective 1 July 1989); for the United Kingdom, the Copyright (Computer Software) Amendment Act 1986; for the United States of America, the Computer Software Copyright Act 1980 amending the Copyright Act 1974 (17 U.S.C. §§ 101, 117). For a comparative overview see *Sieber*, Legal Protection of Computer Data, Programs and Semiconductor Products – A Comparative Analysis with Suggestions for Legal Policy, in: International Chamber of Commerce (ed.), International Contracts for Sale of Information Services, 1989, pp. 7 et seq.; *Vandenberghe*, Bescherming van computersoftware, en rechtsvergelijkend onderzook, 1984.

24 Council Directive 87/54/EEC of 16 December 1986 on the legal protection of topographies of semiconductor products, OJ L 24/36 of 27.01.1987.

European Community to rapidly pass corresponding laws. American "pressure" that was exerted by a strong requirement of mutuality in the American Semiconductor Chip Act was effective in other countries, too. Special laws were enacted in 1984 in the United States of America, 1985 in Japan, 1986 in Sweden, 1987 in Denmark, the Federal Republic of Germany, France, Italy, the Netherlands and the United Kingdom, 1988 in Spain and Austria, 1990 in Canada, and 1991 in Finland.[25] With respect to *databases*, special protection *sui generis* was created and implemented, for example, in Germany in 1997.[26] General improvements of *criminal copyright law* were passed in 1981 in Italy, 1982 in Sweden, the United Kingdom (with additional amendments in 1983 and 1985) and the United States of America, 1984 in Finland, 1985 in Denmark, the Federal Republic of Germany, France and the Republic of China, 1987 in Canada and Spain, 1988 in the United Kingdom, 1993 in Austria, and 1994 in the Netherlands.[27]

---

25 See, e.g., for Austria, the Semiconductor Protection Act (Bundesgesetzblatt 1988/372); for Canada, the Integrated Circuit Topography Act (S.C. 1990, c. 37); for Denmark, the Act on the Protection of Semiconductor Products, Law No. 778 of 9 December 1987; for Germany, the Act on the Protection of Topographies of Micro-Electronic Semiconductor Products of 22 October 1987 (Bundesgesetzblatt I, 1987, p. 2294, as amended 1990); for Finland, the Act on the Protection of Semiconductor Topographies No. 32/1991 of 11 January 1991; for France, the Act on the Protection of the Topographies of Semiconductor Products, Law No. 87-890 of 4 November 1987; for Italy, the Provisions Protecting Semiconductor Product Design of 1987; for Japan, the Act Concerning the Circuit Layout of a Semiconductor Integrated Circuit of 31 May 1985; for the Netherlands, the Act of 28 October 1987 on the Protection of Original Topographies of Semiconductor Products; for Spain Law on the Legal Protection of the Topographies of Semiconductor Products of 3 May 1988; for Sweden, the Act on the Protection of the Layout-Design of the Circuitry in Semiconductor Products, Law No. 1425 of 18 December 1986; for the United Kingdom, the Semiconductor Product – Protection of Topography – Regulations 1987; for the United States of America, the Semiconductor Chip Protection Act of 8 November 1984.

26 See, e.g., for Germany, Article 7 Information and Communication Services Act of 22 July 1997 (Bundesgesetzblatt I, 1997, p. 1870).

27 See, e.g., for Austria, Copyright Amendment Act 1993 (Bundesgesetzblatt 1993/93) as amended in Bundesgesetzblatt 1996/151; for Canada, Section 42 Copyright Act; for Germany, the Copyright Amendment Act of 24 June 1985 (Bundesgesetzblatt I, 1985, p. 1137) and further amendments in Second Act to Amend the Copyright Act of 9 June 1993 (Bundesgesetzblatt I, 1993, p. 910); for France, Law No. 85-660 of 3 July 1985; for Finland, the Copyright Amendment Acts No. 34/1991 of 11 January 1991, No. 418/1993 of 7 May 1993 and No. 446/1995 of 24 March 1995 the Act Amending the Act Relating to Copyright in Literary and Artistic Works (Law No. 442) of 8 June 1984; for Italy, Law No. 406 of 29 July 1981 Concerning Urgent Measures Against the Unlawful Copying, Reproduction, etc.; for the Netherlands, Copyright Act of 7 July 1994; for the Republic of China (Taiwan), the Copyright Law of 1985; for Spain, now newly incorporated in Articles 270 et seq. Criminal Code 1995; for Sweden, Law No. 284 of 19 May 1982; for the United Kingdom, the Copyright Act 1956 (Amendment) Act 1982 of 13 June 1982, the Copyright Amendment Act 1983, and the Copyright, Designs and Patents Act 1988 (which by Section 107 extends liability to a person who "knows or had reason to believe that the article in question is an infringing copy of a copyright work"); for the United States of America, the Piracy and

d. Illegal and Harmful Contents

A fourth wave of reform legislation with respect to illegal and harmful contents started in a few countries in the 1980s, but is expanding rapidly since the triumphant rise of the Internet began in the mid-1990s. Legal amendments adapting traditional provisions on the dissemination of *pornography, hate speech or defamation* to computer-stored data were passed in the United Kingdom in 1994 and in Germany in 1997.[28] Special provisions clarifying the *responsibility of service and access providers* on the Internet were enacted in the United States of America in 1996 and in Germany in 1997.[29]

e. Criminal Procedural Law

For the 1980s, we can also perceive the beginning of a fifth wave of reforms in the field of procedural law. New laws dealing with computer-specific problems of criminal procedural law were already enacted in Australia in 1971, in the United Kingdom in 1984, in Denmark in 1985, in the United States of America in 1986, in Canada in 1986 and again in 1988 and 1997,, in Germany in 1989 and again in 1996, in the Netherlands in 1992 and in Austria in 1993.[30]

f. Security Law

A last group of issues – discussed in particular in the 1990s – concerns the creation of requirements for and prohibitions of security measures. This field

---

Counterfeiting Amendment Act of 24 May 1982 (17 U.S.C. § 506) and the Copyright Act as amended 1980 (17 U.S.C. §§ 502-505).

28 See, e.g., for Germany, Articles 1, 4, 5 and 6 Information and Communication Services Act (Bundesgesetzblatt I, 1997, p. 1870); and for the United Kingdom, Criminal Justice and Public Order Act of 1994 amending the Obscene Publications Act.

29 See, e.g., for Germany, Section 5 of the Teleservices Act (Bundesgesetzblatt I, 1997, p. 1870) as well as Section 5 of the State Treaty of the German Länder on Media Services of 12 July 1997 (cf. Bayerisches Gesetz- und Verordnungsblatt 1997, p. 225); for the United States of America, Sections 501 et seq. Telecommunications Act of 1996 (the provisions are also known as "Communications Decency Act").

30 See for Austria, Strafprozeßänderungsgesetz 1993, Bundesgesetzblatt 1993/526; for Canada, Section 16 Competition Act; Subsections 100 (6) and 101 (5) of the Section 101 (3)-(6) Environmental Protection Act; Section 18 (2) Mutual Assistance Act; Section 487 (2.1.) Criminal Code, introduced by the Criminal Law Improvement Act 1997; for Denmark, chapter 71, Section 780 of the Administration of Justice Act, amended by Act No. 229 of 6 June 1985; for Germany, Article 4 (17s) of the Poststrukturgesetz of 14 June 1989; Sections 90 and 92 Telekommunikationsgesetz of 1 August 1996, Bundesgesetzblatt I, 1996, pp. 1117 et seq.; for the Netherlands, especially Articles 125f-n Criminal Procedural Code; for the United Kingdom, the Police and Criminal Evidence Act 1984.

of law includes minimum *obligations* for security measures in the interest of privacy rights or in the general public interest. It also covers *prohibitions* of specific security measures in the interest of privacy rights or of effective prosecution of crimes (such as limitations of cryptography).[31]

3. The Need for an In-depth Comparative Analysis

Due to the multitude of new legal problems in the field of computer crime, an analysis of all new problems in the above-mentioned six different areas of law is already difficult on the national level: In most national systems, there are no comprehensive overviews on the relevant questions. On the international level, a comparative analysis is even more difficult and respective studies are missed even more since a comparative analysis is a prerequisite for international and supranational solutions. In order to overcome this deficit, the legal chapter of this study (infra chapter III) will elaborate the necessary comparative analysis covering the above-mentioned main areas of computer crime.[32]

C. The International Dimension

1. Driving Forces

Computer data, which is the main object of computer crime, is characterised by an extreme mobility which exceeds by far the mobility of persons, goods or other services: International computer networks can transfer huge amounts of data around the globe in a matter of seconds and thus enabling the commitment of using a computer based in one country with the results surfacing in another.

---

31 These provisions are not included in the terms of reference of this report and therefore will only be dealt with briefly.

32 The legal analysis will not deal with the substantive law problems of all possible computer-related crime such as, e.g., murder or drug dealing assisted by computers, since the respective criminal laws do not depend on the crime being committed with the help of a computer. Due to this concentration on computer-specific legal problems, the legal part of this study on computer-related criminal law will be narrower than the empirical analysis on computer-related crime in chapter II.

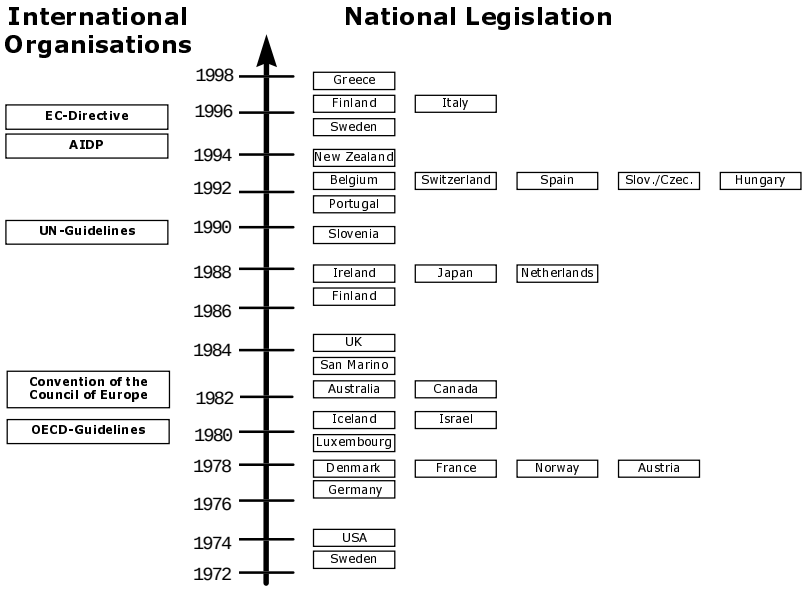
This mobility of computer data in international computer networks makes international solutions for fighting computer crime indispensable: Different national strategies with the aim of preventing computer crime would create "data havens" or "computer crime havens" which, in turn, would lead to market restrictions and national barriers to the free flow of information and Europe-wide services. Above all, national solutions and restrictions for the free flow of information would be doomed to failure since the amount of data transferred in international computer networks makes controls of their content neither possible nor socially desirable. Thus, international and supranational aspects concerning computer crime gain much more importance than in other comparable fields of crime.

2. Main Actors

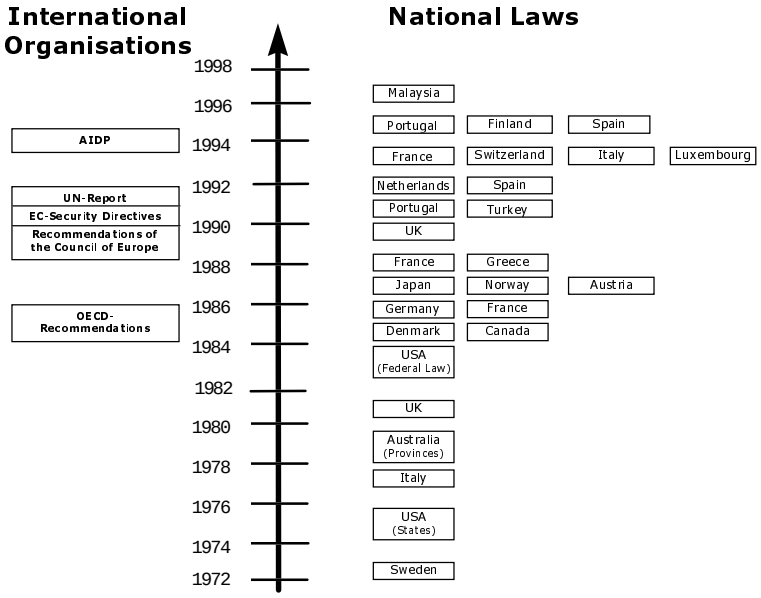
International and supranational organisations have realised these global aspects of computer crime at an early stage and have contributed to the international co-operation and harmonisation in this area of law to a high degree. The main actors in this field have been the OECD, the Council of Europe, the European Union and – recently – the P8 and Interpol. In addition, the UN, WIPO and GATS have also played an important role.

These international and supranational organisations have significantly contributed to the harmonisation of criminal law as well as of underlying civil and administrative law in all of the above-mentioned areas of computer-related criminal law reform. The following graphics illustrate the close interrelationship between the activities on the international and supranational level and the law reform on the main national level. They also demonstrate that already the preparation of the respective initiatives had a considerable impact on national laws by bringing the major national players together. The graphics also illustrate the European Community's power to adopt binding directives, which opened a new age of legal harmonisation in Europe. Furthermore, the graphics show in which areas international and/or supranational activities are still missing or not effective.

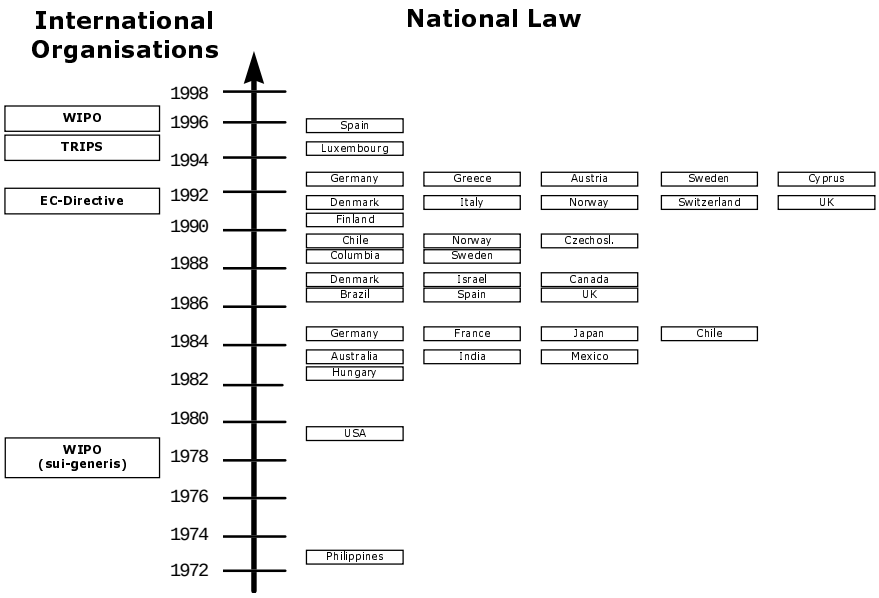
a. Privacy Protection (Primarily General Administrative and Civil Data Protection Law)



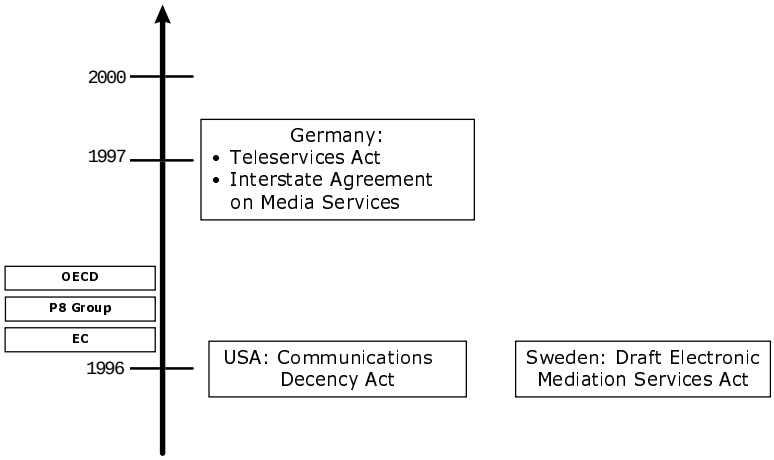
b. Computer-Related Economic Crime



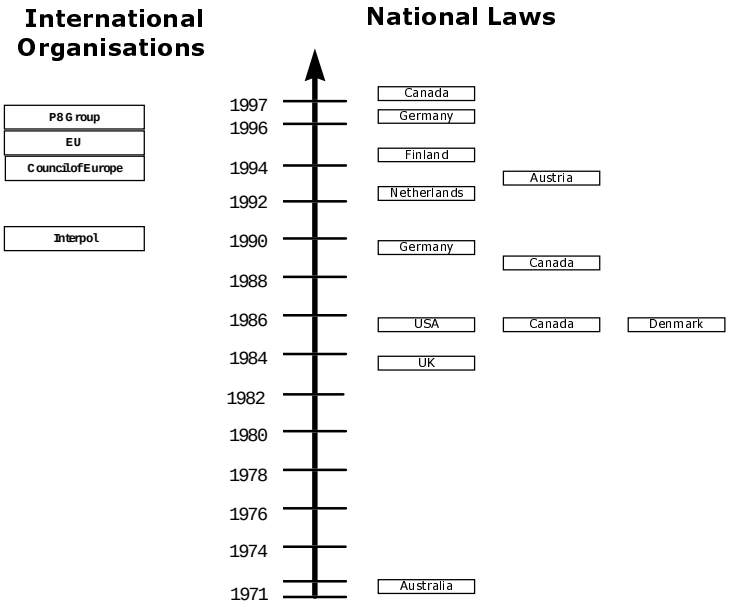
c. Intellectual Property Protection (Using the Example of Copyright Protection of Computer Programs)



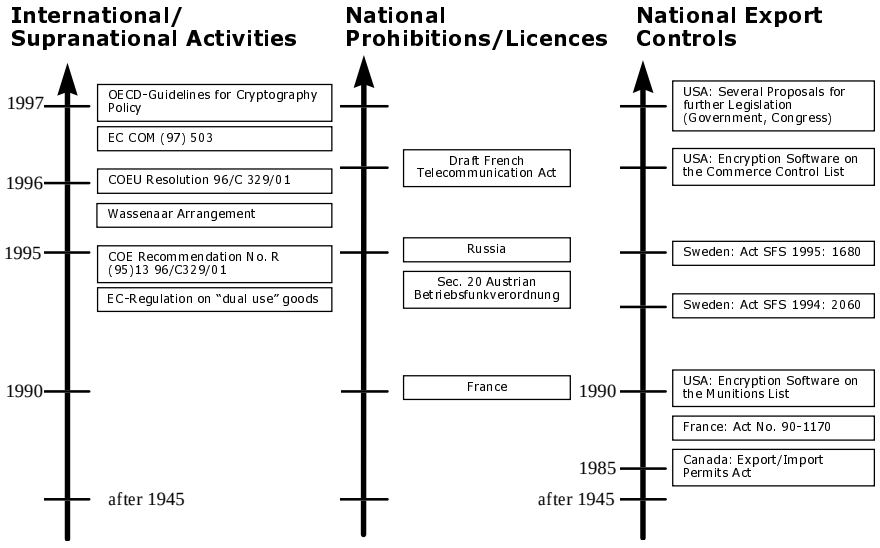
d. Illegal and Harmful Contents (Using the Example of Responsibility of Access and Service Providers)



e. Criminal Procedural Law



f. Security Regulations (Using the Examples of Prohibitions and Export Controls for Cryptography)



3. The Need for a Comprehensive Inventory of International Activities

The graphics above show that the efforts of international and supranational organisations have considerably increased in recent years: Whereas in the 1970s and 1980s, there was a lack of international activities, today there is a lack of co-ordination among the various organisations which risk starting redundant programs. In order to avoid overlapping work of international organisations, a comprehensive inventory of their activities in the field of computer crime is necessary for the future. The present study will provide such an inventory (infra chapter IV), differentiating between the various areas of computer crime legislation. The analysis of these activities will then be the basis for recommending future activities.

D. Finding Solutions

The empirical, the national legal and the international analysis of this introduction show a complex pattern of multiple new forms of crime and new legal problems which up to now have been dealt with independently on a case by case basis. Finding convincing solutions will therefore require to go beyond these single phenomena and to ask for the relevant paradigm shifts behind them. After the empirical and the national as well as the international legal analysis, this study will therefore investigate these fundamental changes before developing new solutions and recommendations. This analysis of paradigm shifts will lead to fundamental principles and to a comprehensive set of measures for fighting computer crime (infra chapter V).

With respect to legal measures of the European Union, the specific question arises whether the European Union has a competence to deal with the legal measures. Consequently, as far as legal measures are concerned, the report will have to first analyse the respective competences under the first and the third pillar of the European Union before suggesting some priority actions for the EU in the legal field (infra chapter VI).

E. Conclusions for this Report

As a consequence of these considerations, the present study will first give an overall view on the development and the current forms of computer crime (infra chapter II). It will then provide a comparative analysis of the relevant legal questions (infra chapter III) and an inventory of the respective activities of international and supranational organisations (infra chapter IV). Finally it will investigate the general aspects for finding solutions, starting with an analysis of fundamental changes and then concentrating on concrete proposals for activities of the European Union (infra chapter V and VI). In an annex the report will present the database (corpus iuris) of computer crime statutes which were collected during the execution of the contract and which might be helpful for the future work in this field (infra chapter VII).

II. The Problem: Current Forms of Computer Crime

In most countries, the discussion about computer misuse began in the 1960s with the endangerment of *privacy*, which was discussed under the headword of "data protection" and was later integrated within the concept of "computer crime" (see infra A).[33] Since the 1970s, scientific research concentrated on computer-specific *economic crimes*, especially computer manipulations, computer sabotage, computer espionage and software piracy (infra B).[34] The rapid growth of the telecommunications sector since the 1980s and especially the spread of the WWW since the 1990s then brought along the dissemination of *illegal and harmful contents*, such as pornography, hate speech and other communication offences in international computer networks (infra C). At the same time, the use of computers and modern communication technology by perpetrators in new fields of crime, e.g. in *organised crime*, made it obvious that there were almost no boundaries for computer-related crime and that – from a phenomenological point of view – homogeneous computer crime no longer existed (infra D).[35] Since the respective modi operandi no longer follow a continuous path, but constantly adapt to new technologies, the following analysis of these four main groups of computer crime will each start with a short description of the historical development and then give an analysis of the present main forms of crime.

A. Infringements of Privacy

While computers began their triumph in the 1960s, it was realised in several western countries that the collection, storage, transmission and connection

33 For the historical development see supra chapter I.A.1.

34 Cf. *Sieber*, Computerkriminalität und Strafrecht, 1st ed. 1977, 2nd ed. 1980, pp. 1/39 et seq., 2/97 et seq. (Japanese translation by *Noriyuki Nishida* and *Atsushi Yamaguchi*, 1986 and 1988).

35 Cf. *Sieber*, The International Handbook on Computer Crime, 1986, pp. 26 et seq. (French translation "La délinquence informatique" by *Sylvie Schaff* and *Martine Briat*, 1990); *Sieber*, The International Emergence of Criminal Information Law, 1992, pp. 6 et seq.

of personal data endangered the personal(ity) rights of citizens. Orwellian visions and the mistrust of the revolting youth of the late sixties inspired the discussion about the dangers of the "big brother". However, during the 1980s, the old pattern of the computer as an exotic instrument in the hands of the powerful became obsolete with the massive spreading of personal computers. It became clear that the protection of privacy within the DP-area also had to consider the multitude of private computer systems and to establish a difficult balance of interests between the privacy interests of data subjects concerned and the economic freedom of the holders of personal data.

These changes can also be seen in the fields of criminal infringements of privacy. According to official statistics, nowadays data protection offences are only of limited importance.[36] The cases that became known show different degrees of endangerment: The misuse of documents of the "Staatssicherheit", i.e. the documents of the Ministry for State Security of the former German Democratic Republic, or the possible blackmailing of AIDS-infected patients prove that in the information society of the 20th century, data protection is a central matter of concern. The storage of information about defaulting debtors by credit investigation agencies or the transmission of data within criminal prosecution authorities illustrate, however, that the ascertainment of criminal infringements of privacy in numerous cases depends on a difficult assessment and evaluation of conflicting principles: The underlying discussion on values and interests does not only have to deal with the protection of privacy, but also with the freedom of information, which is the driving force behind the cultural, economic and political development of an "open society".[37]

> "Clear" infringements of privacy became known especially in the area of traditionally protected professional secrets, especially concerning official secrecy as well as the requirement of confidentiality for officials, doctors, lawyers and banks. Such data constituted the object of the offence in a South-African case, in which the offender – presumably through theft of magnetic tapes – obtained medical data of persons which had undergone an AIDS-test; the confidential data was passed on to the employers of the affected persons.[38]

---

36 In Germany, the share of data protection infringements compared with the total number of computer crime cases registered by the police just amounted to about 1% in 1996. Cf Bundeskriminalamt (ed.), Polizeiliche Kriminalstatistik of 1996, table appendix 01, sheet 20, key figure 7280 as well as *Möhrenschlager*, in: Sieber (ed.), Information Technology Crime, 1994, p. 200.

37 Cf. already *John Stuart Mill*, On Liberty, 1859; *Popper*, The Open Society and Its Enemies, 2nd ed. 1945.

38 Cf. for this case *van der Merwe*, in: Sieber (ed.), Information Technology Crime, 1994, p. 423.

Another clear case of infringement of traditional regulations on protection of secrets happened in 1989 when two employees of one of the biggest Swiss banks helped the French tax authorities to decode magnetic tapes containing customers' data for a compensation of FF 500,000. Similar cases can be found in Germany: A number of new cases of 1996 and 1997 show that perpetrators increasingly try to get hold of banking data in order to blackmail banks with the threat to publish the acquired data (often containing information of tax fraud of the banks' customers).

In contrast, difficult problems on evaluation and assessment with regard to the ascertainment of infringements of privacy are illustrated by an Italian case: In 1986 IBM was accused that its security system RACF represented an inadmissible control over employees.[39] Numerous other cases could be added to illustrate the evaluation problem of infringements of privacy: E.g. in 1994 in Germany the question came up whether the outsourcing of the data processing department of a health insurance company (including the transfer of medical data from the insurance company to the outsourcing company) could infringe traditional secrecy law and data protection laws.[40] Similar problems occur today with respect to the storage of user data for telephone and computer networks: On the one hand, the storage of these data is required or useful for purposes of billing, statistics and criminal investigations; on the other hand, the growing amount of data transferred in international computer networks aggravates the risks of infringements of privacy.

These potential risks of personal data within the Internet today are especially illustrated by the use of executable applets or "cookies". Cookies are text files that store static information about a user's movements on the Internet. The information stored is initiated by specific web servers and generated at the moment the user calls a web page on the server. On reconnecting through web browser software, this information is transferred to a WWW server. Contrary to this, applets can – once activated on the computer – collect system and user specific information and send them independently through a network. The data which is gathered this way is often used to send mass bulk e-mails – a phenomenon called "spamming". In many cases these activities and especially the transfer of the Internet user's personal data are executed without the user's consent or knowledge.

B. Economic Offences

Since the 1970s, the discussion about computer misuse was not only marked by infringements of privacy but also by computer-related economic crimes, which today are regarded as the central area of computer crime and which were at first exclusively characterised by that term. During the 1970s, fraudulent computer manipulations were the starting point of the discussion about computer-related economic offences and the core centre of computer-related economic crime. However, today hacking has increasingly

39 Cf. for the last two cases *Sieber*, The International Handbook on Computer Crime, 1986, pp. 23 et seq.

40 Case not published (from the private consulting of the author).

become a "basic offence" which is then used to commit acts of espionage, software piracy, sabotage as well as computer fraud.

1. Computer Hacking

The term "computer hacking" traditionally describes the *penetration of computer systems*, which is not carried out with the aims of manipulation, sabotage or espionage, but for the pleasure of overcoming the technical security measures. In practice, this kind of offence can be frequently found.[41] As far as the damage of these cases is concerned, a differentiation is essential: In numerous cases, the penetrated computer user is not actually harmed, but only endangered. However, in these case, too, the "formal sphere of secrecy" or the integrity of the concerned computer systems is violated. Contrary to this, considerable damages occur in other cases especially when the perpetrators later use their knowledge for committing espionage, sabotage or fraud.

> One of the most severe cases of sophisticated "hacking" involved a group of German teenagers in the late 1980s. They had managed to get access to various American computer systems and then sold the knowledge obtained in their data journeys to the former Soviet secret service KGB. The case was discovered because one of the hackers sought help at the author's former Bayreuth chair, leading to a deal with the prosecution authorities: The hacker revealed his knowledge and the investigation against him was turned down. The case was of particular interest because information on new techniques of computer manipulation were revealed in the course of this proceeding.[42]

The techniques of hacking highly depend on the respective communication system. "Traditional" forms of hacking in computer networks were developed during the 1980s based, e.g., on the insecure use of standard passwords (which are often not changed regularly by the computer users). Although the understanding of computer security and the handling of passwords have improved since then, in recent years the Internet has

---

41 In a Dutch statistic of 1991, the cases of hacking amount to approximately one fifth of all computer crimes. Cf. *Kaspersen*, in: Sieber (ed.), Information Technology Crime, 1994, p. 347 (with explanations about the groups of crimes on p. 345). The twilight zone of hacking is very large, because the respective attempts of getting access often cannot be registered and traced back.

42 Cf. for this case *Hafner/Markoff*, Cyberpunk, 1991, pp. 139 et seq. The resolving of this case confirms the effectiveness of a "self-revelation" for cases of hacking already called for before, cf. *Sieber*, Informationstechnologie und Strafrechtsreform, 1985, pp. 54 et seq.

brought along new techniques of computer manipulations, such as IP-,[43] DNS-[44] and web-spoofing,[45] or infiltration of computer networks by malicious web applets.[46] These methods evolved out of the use of new communication protocols like the Internet Protocol (IP) or the Hypertext Transfer Protocol (HTTP) used to run web servers.

Due to recent developments in the field of telephone and telecommunications technology (such as ISDN), hacking does not only affect classic computer systems but also increasingly *telephone lines*, answerphones and voice-mail-systems. "Telephone hackers" dial themselves into the telephone companies local phone exchanges and are thus able to eavesdrop on the digitally led conversations in a respective part of town.[47] In the US, besides other confidential information, especially the numbers of telephone access cards (so-called calling cards) are eavesdropped on, which are then resold.

An example for the new form of telephone hacking is a case of 1992: Young Germans penetrated the speech computer of the Barclays Bank in Hamburg to which the clients of the bank reported the receipt of their credit cards including the corresponding secret personal identification numbers as well as announcements in case of loss or – by

43 The technique of IP-spoofing is used to gain unauthorised access to computers or networks from outside by pretending to be an authorised and trusted device inside the penetrated network. This is done through modification of IP addresses in data packet headers transmitted to an incoming port of the network's router. Although the fake IP address is known as a valid address inside the network only, routers were not able to distinguish between data transmitted from outside or inside of network. Newer routers and firewalls offer protection against this kind of attacks.

44 DNS spoofing describes the faking of hostmasks during the resolution of internet hostnames. DNS or "Domain Name Service" provides the mapping between hostnames and IP addresses. Every access request on the Internet using the host's name has to be resolved to its IP address, which is done by communicating with a DNS-server which stores the hostmasks in databases. To perform the DNS spoofing attack, a hacker tries to intercept the communication and to send fake hostname mappings to the victim's computer. This can easily be done using malicious web applets downloaded by the attacked user himself. Once the applet is activated, the user's communication could be rerouted and the transmitted data could be gathered. Also cf. <http://www.heise.de/ct/art_ab97/9710286/> (accessed on 22 January 1998).

45 While IP- and DNS-spoofing depend on sophisticated technical knowledge, web-spoofing attacks use a much simpler approach. These are based on optical illusion in general. Hyperlinks on web pages can contain characters that make an address look real, but in fact lead to a wrong web site, e.g. replacing the letter "o" in the address <www.microsoft.com> for the number "0" could result in the address <www.micr0s0ft.com>. Most users would not suspect any malicous intention. In this example, the hacker would set up a web page asking for the input of sensible user information, e.g. credit card information.

46 For more information on the security of Java: <http://semcoe.wmg.warwick.ac.uk/javadocs/javasecurity.html> (accessed on 22 January 1998).

47 Cf. "Focus" No. 17/1993, p. 106.

giving the respective secret number – when asking for an increase of their credit limits.[48]

2. Computer Espionage

Computer espionage – only rarely appearing in official statistics[49] – constitutes a special danger compared with traditional economic espionage, because in computer systems, huge quantities of data are stored in an extremely narrow space, and the data can be copied quickly and easily with the help of modern technology, also via data telecommunication. The objects of offence are especially computer programs, data of research and defence, data of commercial accounting as well as addresses of clients. As the modus operandi, the simple copying of data is predominant; the theft of data carriers, the evaluation of "remaining data" or the absorbing of electromagnetic emissions are also effected. Besides young hackers and competing business enterprises, secret services increasingly appeared to be dealing with economic espionage in recent years.

The case of the "KGB hacking" presented above illustrates the close relation between hacking and computer espionage. A Japanese case from 1988 shows the possibility of using computer viruses for computer espionage: In this case, a computer virus penetrated a network of personal computers, collected secret numbers of other network users and then wrote these numbers down on a internal network "black board" in an encoded form usable only for the perpetrators.[50]

With the convergence of data processing and telecommunication as well as with the digitalisation of telecommunication, the line between traditional computer espionage and *telephone fax and e-mail monitoring* becomes increasingly blurred. In the case of telephone tapping, the criminals today penetrate the telephone exchanges of the telephone companies especially via normal data lines. Car phones, directional radio stations and satellite connections are particularly easy to attack in case of uncoded communication.

Giving an example for potential impact of such activities, reliable sources in Germany refer to the competition between the German company Siemens and a French competitor with respect to a huge contract deciding on a future high-speed train system in South Korea: French agents could intercept the satellite based fax

48 Cf. "Der Spiegel" No. 34/1992, pp. 206 et seq.

49 According to the Polizeiliche Kriminalstatistik 1996, less than 3% of computer crime cases can be assigned to computer espionage. See also: *Möhrenschlager*, in: Sieber (ed.), Information Technology Crime, 1994, pp. 200 et seq.

50 Cf. *Yamaguchi*, in: Sieber (ed.), Information Technology Crime, 1994, p. 307.

transmission of the offer of the German company which was not encrypted so that the French company could undercut the German offer.

The techniques of bugging telephones were used especially by the State Security Service of the former German Democratic Republic: The telephone numbers of politicians, of members of the secret service and of other important bearers of secrets of the Federal Republic of Germany were registered as target numbers, so that the telephone communications of these persons were automatically recorded.

Massive measures of listening in on telephone conversations are/were also carried out by the American National Security Agency (NSA). According to published reports, the NSA is said to run more than 2,000 installations for bugging telephones world-wide, which can supervise up to 54,000 telephone conversations at the same time.[51]

3. Software Piracy and other Forms of Product Piracy

The unauthorised copying and use of *computer programs* – often called theft of software or software piracy – at first involved, in accordance with the historic development of computer technology, the copying of individual software which frequently contains important internal company know-how. Therefore software theft overlaps with computer espionage in many cases.

The German "debit collection program case" is an example for the copying of individual software which led to the first decision of the Bundesgerichtshof concerning the possibility of copyright protection: Because of the copying of its central computer program and the following low-price sales by the perpetrator, the victimised debit collection company got into a situation that threatened its existence.[52]

Nowadays standard software is sold on a massive scale, and as far as the number of crimes are concerned, presently the predominant offence is the illegal copying of standard software especially for the use on personal computers. Just how wide-spread this phenomenon is was shown by the fact that in Europe, on average only 0.5 computer programs were sold per personal computer in use.[53] The industrial organisation "Business Software Alliance" estimated the market share of illegally copied software at, e.g., 40% in the USA, 76% in Germany, 81% in Japan and 98% in Thailand.[54] Therefore, the total damage of software piracy is very high.[55]

---

51 Cf. *García*, 38 (1991) UCLA Law Review, pp. 1043 et seq. (at p. 1055).

52 Cf. *Sieber*, Bilanz eines "Musterverfahrens" – Zum rechtskräftigen Abschluß des Verfahrens BGHZ 94 276 (Inkassoprogramm), (1986) Computer und Recht, pp. 699 et seq.

53 Cf. also *Schick/Schmölzer*, in: Sieber (ed.), Information Technology Crime, 1994, p. 30.

54 Cf. "Newsweek" of 29 June 1992, pp. 44 et seq.

55 E.g., in Austria, the total damage caused by software piracy (without damages caused by violations of semiconductor protection) is estimated at schilling 3,000 million: Cf. *Schick/Schmölzer*, in: Sieber (ed.), Information Technology Crime, 1994, p. 30. In Canada, the losses caused by software piracy are estimated at US$ 200 million: Cf. *Piragoff*, in: Sieber (ed.),

A German case from 1994 shows the high resulting damages and also illustrates the careless handling of security measures by program distributors and the proneness of new forms of distribution to misuse: During the biggest German computer fair, a software dealer had distributed about 200,000 free copies of a CD ROM, which contained programs worth more than DM 100,000. Each program was code protected which should only allow the CD-user who concluded a contract to gain access to the program. However, young hackers succeeded in "cracking" the code and the program protection of the CD ROM and passed the code on to the visitors on the same fair.[56]

Software piracy in the field of standard programs does not nearly represent a trivial offence of young PC-users. The software industry now increasingly takes legal action against enterprises that use unlicensed software. In these cases, often only a fraction of the installed programs are licensed. For example, during a police search at a company in northern Germany, the police found that only nine out of 58 installed programs of which were licensed.[57] In this case, a fine of DM 100,000 was imposed for further licenses and compensation for damages.

During the 1990s, the distribution forms of software piracy changed: The illegal sale of computer programs that dominated in the 1980s was considerably reduced due to the corresponding prosecution practices applied in this field. At first, the most frequent new forms of distribution had been the sale of programs in so-called "ant trades" at flea markets (which were run and organised by professional gangs).[58] Moreover, the practice of software piracy had been characterised by dealers who produced and sold illegal copies of standard software in large numbers. These software packages were often distributed as an extra supplement to the original hardware.[59]

Today the Internet plays the dominant role in the illegal distribution of software and other protected products. Users with writing access to FTP or web servers, whether official or by hacking, create hidden directories to collect and store huge amounts of illegal copies of commercial software. They use all kinds of online communication facilities, like e-mail or bulletin

---

Information Technology Crime, 1994, p. 87. In Germany, the Union of the Software Industry estimates a business loss to the extent of US$ 1.5 billion due to Far Eastern illegal copies: Cf. "Handelsblatt" No. 2 of 3 January 1995, p. 1. Therefore the share of software piracy in computer crime is very high: In Germany, it amounts to more than 10% in 1991 and to almost 10% in the Netherlands. Cf. for the corresponding statistics *Möhrenschlager*, in: Sieber (ed.), Information Technology Crime, 1994, pp. 200 et seq.; *Kaspersen*, in: Sieber (ed.), Information Technology Crime, 1994, p. 347 (with explanations about the groups of crimes on p. 345).

56 Cf. *von Gravenreuth*, Neue Formen der Softwarepiraterie, (1995) Computer und Recht, pp. 309 et seq.

57 Cf. "Handelsblatt" of 7 November 1994, p. 16.

58 Cf. *von Gravenreuth*, Neue Formen der Softwarepiraterie, (1995) Computer und Recht, pp. 309 et seq.

59 Cf. for Canada Piragoff, in: Sieber (ed.), Information Technology Crime, 1994, p. 87.

boards, to spread – using secret language codes – the message for download options. Moreover, the software is usually stored only for one hour, thus making it almost impossible to allow prosecution due to lack of traces.

> As a consequence, the Australian Performing Rights Association (APRA), the collecting society for the Australian music industry, has brought a Federal Court action against OzEmail, Australia's biggest Internet service provider in March 1997. APRA claims that OzEmail infringes copyright by transferring music files to their subscribers via the Internet.

The high value of data in the information society leads to the fact that besides the illegal use of computer programs, also *databases* and other data collections are increasingly used illegally. Today the illegal copying of data (characterised as "downloading") affects both the hosts of online databases as well as the distributors of offline-databases.

> In Germany a number of court decisions concerned, e.g., the sale of CD ROMs with telephone numbers and addresses. In some cases the perpetrators only copied the relevant data by computers, in other cases the data was retyped in China in order to avoid legal remedies for illegal copying (which proved to be unsuccessful). In the following court proceedings the relevant cases were not only dealt with on the basis of illegal competition but also as infringements of privacy rights of telephone users.[60]

With respect to traditional *cultural works of authorship*, the convergence of data processing and data communication as well as the digitalisation in the distribution of cultural products (e.g. the sale of compact discs with music and movies) show the common roots of software, music, video and multimedia piracy in the "informatised" society.[61] The connections between software piracy and other forms of product piracy become evident with emerging new devices for playing and producing compact discs which, in the age of "multimedia", contain computer programs, databases, books, music and television movies.

> The threat of computer technology and especially the Internet to the traditional press media was illustrated when the book "Le grand secret" of Dr. Claude Gubler, the physician of the former French State President Mitterand, was scanned, translated and published on the Internet, although prohibited in France. In this book Mr. Gubler claims that State President Mitterand was suffering from cancer right from the beginning of his governing period.

---

60 See Oberlandesgericht Karlsruhe, (1997) Neue Juristische Wochenschrift – Computer Report, pp. 352 et seq.

61 Cf. for this also *Braun*, Produktpiraterie, 1993, pp. 11 et seq., and Produktpiraterie, (1994) Computer und Recht, pp. 726 et seq.

4. Computer Sabotage and Computer Extortion

The high concentration of data stored in the electronic devices mentioned above, along with the dependence of many companies and administrative authorities on DP, make computer sabotage another particular danger for business and administration. The objects of computer sabotage are the tangible computer facilities as well as the intangible data containing computer programs and other valuable information.

For the *modi operandi*, one can be differentiate between methods causing physical damage and those causing logical damage. During the 1970s, the most frequently practised methods of causing physical damage were igniting or bombing a building. These techniques were typically applied by "outsiders" not employed or otherwise related with the owners of the facilities damaged.

> For "insiders" aiming to affect facilities within the company mainly in cases of labour and other social conflicts, the following additional techniques of physical destruction were recommended by left-wing European underground magazines: gluing emery paper onto the electronically readable parts of cards in order to destroy badge- or card readers; inserting iron-cuttings, paper clips, or small pieces of aluminium foil into computer devices in order to cause electrical shortcuts; pouring coffee, saline solution, and caustic cleaning agents into the operator console and other equipment; blowing smoke, hair-spray, and other gases into sensible devices; putting a container of hydrochloric acid in front of the air-conditioning's induction pipe or suction fan; causing extreme temperatures by sabotaging the air-conditioning or by heating computer parts with a lit cigarette; interfering with the electric power station, switching office, or communication lines; and cutting cables or putting mice under a raised floor where they could gnaw through the insulation of electrical power-cords.

Today, the most popular method of causing logical damage is through the use of crash programs which can erase large volumes of data within a short period. These programs can be self-written utilities or "Trojan-horse" routines built into application programs or into the operating system. Crash programs can also exploit hardware and software defects ("bugs").

> An example of computer sabotage by using computer programs to erase data is the case involving a southern German engineer. He erased the comments of a valuable computer program on the disc before leaving the company so that it could not be easily modified by other programmers due to which the company almost lost a contract worth about DM 1 million. The accused programmer declared that he had copied the comments onto another disc in order to save space on the original one, and that the second disc must have been lost after his dismissal.

Special problems are caused by the wide diffusion of virus and worm programs. Computer viruses are programs which spread in computer systems and – possibly with a delay of time – often cause damages. These programs are distributed especially through software piracy and the use of networks. As a consequence, cases involving viruses constitute a

considerable share of total numbers in computer crimes.[62] The variety of viruses in circulation has increased in recent years. In some cases, the original software which was issued by the producing company was already infected with a virus. While viruses only spread in "host programs", worm programs attack other computer systems independently.[63]

An illustrative example for the possible dangers is the American "Internet worm"-case. In this case a young computer scientist created an extremely complex virus which consisted of several programs. The virus was injected into a Department of Defence research computer system. Due to a design error it replicated wildly in a similar manner as a worm, ultimately jamming more than 6,000 computers. Although the virus caused no actual damage to any files, it cost many thousands of employee hours to locate and erase this virus.

In recent years, the technical design of these viruses became evermore sophisticated, thus enhancing the spreading of viruses and making their prevention more difficult. This can be seen especially in the fields of so-called boot sector and macro viruses.

Boot sector viruses began plaguing users' personal computers during the early 1990s. This type of virus is able to destroy – once copied to a storage medium like floppy or hard disk – the file allocation information. Contrary to viruses that become activated through loading an executable file, boot sector viruses already spread by insertion of a floppy disk to a drive and the following exchange of floppy disks.

Macro viruses which have emerged since 1996 are based on the fact that standard applications like word processors and spreadsheets have become more and more sophisticated. Giving the user the ability to add programming codes directly into document files to automate different tasks, this feature of macro programming is increasingly being abused to develop new types of viruses. Up to this point, only executable binary files were believed to be proper carriers of malicious virus data. However, by adding the feature of macro development, formerly harmless files can now delete file contents or activate hidden processes simply by being opened. Thus the macro viruses use the application's built-in program functionality to replicate to other files stored on the computer. Macro viruses got widespread through the exchange of document files on floppy disks and the sending of e-mail attachments.

A new phenomenon is the abuse of faulty hardware or software implementation (so-called "bugs") to crash computer programs or computer systems.

In 1997, this was especially illustrated when computers which run on specific version of the Intel Pentium chip were caused to crash while executing programs containing

62 In the Netherlands, statistics for computer viruses reveal that these cases of sabotage amount to almost 30% of the total number of computer crimes. Cf. *Kaspersen*, in: Sieber (ed.), Information Technology Crime, 1994, p. 347 (with explanations about the groups of crimes on p. 345).

63 Computer worms can therefore be defined as computer viruses which spread not only in a computer system but in computer networks and which infect a multitude of computers.

special machine code commands.[64] A similar phenomenon is the "ping of death", which happens when a simple and customised program based on the common ping[65] utility sends specific data to Windows 95 systems and causes them to halt due to a conceptional error in Window's TCP/IP software implementation.

Normally, these kinds of attacks do not entail permanent damages to the system which will work again after a system reset. Unsaved data, however, is usually lost without the chance of recovery. The manufacturers of the affected devices or software usually develop so-called "bug fixes" or "workarounds" to prevent such forced crashes. Nevertheless, the rapid development of technologies especially leads to a situation where potential offenders will always be at least one step ahead.

The above-mentioned convergence of computer and telecommunication systems leads to the situation where physical acts of sabotage are increasingly being directed against telephone and other data lines, too. In the field of computer sabotage, the same development as in the sphere of the above mentioned cases of hacking and espionage is occurring.

An example for sabotage in the field of data lines was an attack on the network of Deutsche Telekom in February 1995: The offenders cut seven underground optic fibre cables and thus interrupted approximately 7,000 telephone and data lines around Frankfurt/Main airport. In a letter a group called "Keine Verbindung e.V." claimed responsibility and declared that they had tried to disturb the deportation of persons seeking political asylum.[66]

Cases of computer sabotage constitute a serious problem especially due to the fact that the economy, the administration and frequently also the individual citizen depend to a high degree on the functioning of modern computer and communication systems.[67] This dependency of the information society on computer systems also makes computer extortion a dangerous

---

64 A newly found bug in Intel Pentium processors is now being discussed on the Internet. The "Pentium F0" bug can crash Pentium MMX and "classic" Pentium (non-MMX) computers, cf. <http://www.dgl.com/dglinfo/1997/dg971108.html>, <http://support.intel.com/support/processors/pentium/ppiie/> (both accessed on on 22 January 1998).

65 The program "ping" is used to determine whether an Internet host is reachable at a certain moment and for how long the data travels over the Internet. See for further details <http://www.sophist.demon.co.uk/ping/> (accessed on 22 January 1998).

66 Cf. for this "Frankfurter Allgemeine Zeitung" No. 28 of 2 February 1995, p. 1 and No. 29 of 3 February 1995, p. 1.

67 This dependency also leads to the high total damages which in different statistics are described as a consequence of computer breakdowns. Thus the total damage which occurred in Austria for private enterprises due to computer breakdowns in 1988 amounts to schilling 1,500 million, cf. *Schick/Schmölzer*, in: Sieber (ed.), Information Technology Crime, 1994, p. 22. In France the corresponding total damage adds up to FF 10,400 million in 1991, of which 5,900 millions are caused by wilful damage actions, 2,700 millions are caused by accidents and 1,800 millions are caused by false operations and programmings, cf. *Francillon*, in: Sieber (ed.), Information Technology Crime, 1994, p. 173.

form of attack. In these cases, the victim is threatened e.g. with the destruction of his computer systems or with the dissemination of secret information.

An example for such a computer extortion is the case of an American scientist who distributed more than 20,000 floppy disks which supposedly contained information about the AIDS-virus, but instead encoded the user's hard disk when opening the stored files. By a corresponding announcement on the screen, the users were asked to transfer an amount of at least US$ 189 to a bank account in Panama in order to obtain the code for decoding the hard disk.[68]

Regarding the threat to disseminate confidential data the German cases mentioned-above can be referred to. In the particular cases banks were blackmailed by the threat to publish customer data (including data of customers who had presumably committed tax fraud offences).

5. Computer Fraud

During the era of large mainframe computers, fraud committed by computer manipulations constituted a uniform group of crimes. Due to the diversification of computer systems in the 1980s, nowadays the term computer fraud describes a spectrum of various cases within the field of economic crimes.[69]

Among the *"classic" large-scale computer fraud cases*, invoice manipulations concerning the payment of bills and salaries of industrial companies as well as the manipulations of account balances and balance sheets at banks were and still are the predominant offences. In addition to this, an extension of manipulations to increase the inventory could be perceived due to the recession of the recent years.

In Germany, a complex invoice manipulation was committed as early as 1974 by a programmer who carried out salary manipulations worth over DM 193,000 through changes of the salary data as well as the book-keeping and balance sheet programs of his company. Using a program written especially for this purpose, he entered the information on the salaries of fictitious people into the data memories containing company salary information and entered his own account as the account to which the fictitious salaries should be transferred. These salary manipulations would have been discovered by the company because normally, the computer prepared wage-slips, checklists, account summaries, and balances sheets which were carefully checked. In order to prevent discovery by these control printouts, the offender first made adjustments in the salary payments program to ensure that no pay-slips were printed for payments to the fictitious employees so that the payment did not appear in the checklists produced by the computer. By further manipulation of the program which produced the company's accounting summaries and balance sheets, the perpetrator

68 Cf. for this case *Kaspersen*, in: Sieber (ed.), Information Technology Crime, 1994, pp. 351 et seq.

69 For computer manipulations outside economic crime cf. infra chapter II.D.

finally succeeded in having the embezzled amounts deducted from the income tax to be paid to the tax office. Thus, the sums did not appear as deficient amounts in the company's accounting summaries and balance sheet.

Among balance sheet manipulations, especially the case of the German Herstatt Bank of 1974 must be mentioned, in which balances totalling over DM 1 billion were manipulated. The modus operandi of the crime was based on keyboard manipulation of the computer responsible for entering the bank business.[70]

The connections of computers to international telecommunication networks soon opened possibilities to commit these computer manipulations from outside the victimised companies. First cases of *online manipulations* became known in the USA during the 1970s. Today most big companies are connected to the Internet and other computer networks. As a consequence the Internet is increasingly used to commit online manipulations. Frequently, the perpetrators take advantage of insufficient security measures in computer systems, lacking or non-adequate use of firewall systems or the inexperience of system administrators of corporate networks. Moreover, the lack of technical experience is widespread among the growing number of individual users which have only recently begun to use online communication.

Numerous misuses of *ATM-cards and similar means of payment* have been added to the total of manipulations since the end of the 1980s. Even though these misuses often only lead to minor sums of damage, statistics indicate that the misuse of cards surpass the number of classic manipulations by far and meanwhile constitute the most frequent computer crime cases.[71] The protection of the respective cards – above all by chip technology – has gained more importance in particular because of the introduction of point-of-sales-systems. Suitable methods of protection are important, regarding the fact that meanwhile, the relevant "classic credit card crime" is committed mostly by organised groups of criminals.

Today the forms of committing misuses of ATM-cards range from the simple use of stolen cards and the manipulation of these with the help of computers to the independent manufacturing of card copies. Apart from ATM-cards, other magnetic cards are manipulated, e.g., phone cards or cards for horse betting.[72]

70 Cf. for the last two cases *Sieber*, Computerkriminalität und Strafrecht, 2nd ed. 1980, pp. 58 et seq., 61 et seq.

71 For detailed statistics see supra I.A.2.a.

72 Cf. *Yamaguchi*, in: Sieber (ed.), Information Technology Crime, 1994, p. 307.

The offenders often obtain the necessary PIN-code for the use of the cards by a phone call trick, by preparing (and manipulating) the keyboard, by using a false keyboard or – as in a Japanese case – by bugging data telecommunication lines.[73]

A Hungarian case was particularly remarkable due to the high sum of damage. Within one month, the respective maximum amount of approximately US$ 250 was withdrawn with the help of the copy of a single card in 1,583 cases.[74]

The misuse of the *telephone network*, a field in which considerable qualitative changes have emerged in recent years, has also evolved into a "mass crime": In the 1960s, offenders wanted to avoid expenditures for their own phone calls only. Since the end of the 1980s, the techniques originally developed by young hackers were also used by "companies" which – in often changing apartments or with the help of mobile telephones – offered conversations especially for intercontinental telecommunication. In the 1990s, even financial manipulations resulting in the transfer of money were made possible by telephone companies when the insufficiently protected telephone network (which had not been developed for this purpose) was used in a careless way for the accounting of services.

Blue boxing was already developed in the 1960s and is based on the fact that in the traditional analogous telephone network, control tones for establishing a link are transmitted through the same line as the information and can therefore be manipulated with the help of the so-called "blue box". By using a telephone number free of charge (in Germany a 0130-number), e.g., an operator of an American telephone company is called. Then the conversation is ended with the help of a "break tone" and the free line is held with the help of a "seize tone". After the input of certain control impulses, it is possible to dial the desired number in the USA free of charge. However, due to so-called frequency blockers, the blue boxing technique now only works in a limited way, i.e. in telecommunications between certain countries only.

Therefore young telephone hackers today predominantly use manipulation techniques which allow phone calls at the expense of other network participants. This is made possible by breaking into inadequately protected voice-mail-systems, where the direct-dialling functions are exploited. Another form of widespread manipulation is the trade with foreign calling card numbers, which, e.g., are being sold by insiders of the telephone companies, who obtained them with the help of trick phone calls from the card holders. These calling card numbers are "hacked" by intruding a computer or by eavesdropping on phone calls. Some of the phone calls are carried out at the expense of other users with the help of modified walkie-talkies or home-made devices.

Apart from that, phonecards for public phone-boxes are faked or manipulated. These manipulations can easily affect countries where only magnetic strip systems are used. In other countries as in, e.g., Germany, the telephone companies use phonecards with integrated chips which are especially secured against "recharging" by hardware

73 Cf. for the Japanese case *Yamaguchi*, in: Sieber (ed.), Information Technology Crime, 1994, p. 307.

74 Cf. for this case *Kertész/Pustazai*, in: Sieber (ed.), Information Technology Crime, 1994, pp. 251 et seq.

protections. However, German youths succeeded to copy these phonecards. They decoded the signals of the cards by using adapter cables and small computers which then simulated the signals with their own "intelligent" cards. The first successful "copying" of a phonecard with a integrated rechargeable chip was completed in Germany in 1994.

Regarding the background of these forms of misuse one could foresee that the use of the telephone network for the accounting of services had to lead to a new wave of manipulations in the 1990s. In Germany, especially the "sex telephones" and "party lines" were used for this purpose, which can be called under the area code of 0190. Out of the DM 1.15 per minute to be paid to Deutsche Telekom, 52% remained with Deutsche Telekom whereas 48% went to the providers of these services (where they were divided between the provider of the service and the provider of the content); for foreign numbers, the revenue per minute amounted to over DM 3. The perpetrators set up – partly with the help of specialised agencies – corresponding service numbers which were then called at the expense of Deutsche Telekom – and of some clients by young telephone hackers who shared the profits. In doing this, they used the whole range of possibilities of misuse described above. Moreover, Deutsche Telekom got harmed even worse when whole private offices were rented for the exclusive purpose of calling chargeable service numbers during a two-month period with the help of numerous (in a particular case up to 400) telephone connections and by using telephone computers before Deutsche Telekom claimed the outstanding invoices. Employees of Deutsche Telekom also misused telephone connections not yet given out to clients by switching off the meter. Furthermore, clients of Deutsche Telekom were also charged when so-called "diallers" (i.e. electronic dialling machines, about the size of a cigarette box and distributed at DM 150) were arbitrarily connected to some switches, local telephone exchanges or wires, which called up pre-programmed numbers especially at night at the expense of the dialled telephone connection.

The first larger inquiries about telephone misuses were carried out in Germany in 1994 when the apartments of 60 suspects were searched in nine German regions at the same time, which lead to the arrest of four persons. Two employees of Deutsche Telekom were arrested who were suspected of having collaborated with foreign organised crime groups. It is estimated that more than 80% of the turnovers off all sex-phones result from such manipulations. According to their own words, some youths obtained monthly commissions of more than DM 100,000. The total damage for Deutsche Telekom and their affected clients is estimated at more than DM 100 million for the year 1994.[75]

Another technique for illegal profits through telephone sex-lines was discovered in Canada and the USA: Over 38,000 users could be convinced to download a picture viewer of several sex sites for free. The software enabled the user to view pornographic pictures over the Internet while seemingly not being charged for the service. However, as soon as the user had started the program, it silently disconnected the users from their local Internet service provider, and reconnected them to the website rerouting the phone call to a telephone sex service in Moldova, first. As a

75 Cf. "Die Welt" of 19 March 1994, p. 12., as well as "Frankfurter Allgemeine Zeitung" No. 289 of 13 December 1994, p. 22 and No. 5 of 6 January 1995, p. 4; "Focus" No. 50 of 12 December 1994, pp. 244 et seq. The German Telekom reacted to the shown cases with measures of public security of which the essential parts are individual invoicing, special warning reports in case of an increase of the telephone costs and the setting up of a centre for network security in Darmstadt; cf. "Computer Zeitung", No. 3 of 19 January 1995, p. 6.

result consumers were billed more than US$ 2 per minute by their long distance providers. After shutting down the picture viewer or web browser, the software kept the modem connected to Moldova, resulting in some long distance telephone calls totalling several thousand US dollars.

Today, the widespread use of the Internet has not only opened a door for the above-mentioned new ways of computer manipulation, but is also creating a new wave of general consumer fraud, e.g. by false advertisement, pyramid scams or illegal gambling.

In 1997 a US Federal District Court sentenced the publisher of a daily financial newsletter to a prison term for conspiracy to commit securities fraud. The publisher of the newsletter had systematically published favourable coverage of stock issues in exchange for economic benefits without disclosing this fact in his international financial newspaper.[76]

C. Illegal and Harmful Contents

In the late 1980s, first cases occurred in which information glorifying violence or information of racist content was distributed with the help of computers especially by political extremists.

In the USA, the Ku Klux Klan, the White Aryan Resistance, skinheads, and other neo-nazi organisations had already realised in the 1980s that it was much more effective to work with means of electronic communication than with traditional "newsletters". These groups used electronic communication systems mainly to distribute the names of Jewish "opponents" and to give advice for violent actions.

In Germany, right-wing and left-wing extremist organisations first used Bulletin Board Systems (BBS) and other electronic communication systems at the beginning of the 1990s. Right-wing extremist organisations especially used the so-called "Thule-Network", which consists of about 10 BBSs. In these BBSs, information about neo-fascistic organisations and corresponding propaganda material was stored. The electronic means of communication were used for the communication within private groups of users as well as for informing the public. Left-wing radical groups (particularly from the anarchistic autonomous scene and from the sphere of the so-called Red Army Fraction) distribute their plans of action especially via the BBS-network "Spinnennetz (cobweb)", which is included in an international exchange of information via the "European Counter Network (ECN)".[77]

---

76 LABnews September 1997, p. 4 (No. 4).

77 Cf. Anti-Defamation League of B'nai B'rith, Hate Groups in America, 1988; *Maegerle/Mletzko*, Terrorism/Extremism/Organized Crime 1994, No. 5, pp. 1 et seq.; Federal Ministry of the Interior (ed.), Report of the Protection of the Constitution 1993, p. 23, pp. 147 et seq.; *Möhrenschlager*, in: Sieber (ed.), Information Technology Crime, 1994, p. 108; *Werthebach*, Lage der inneren Sicherheit aus Sicht des Verfassungsschutzes, (1994) Nordrhein-Westfälische Verwaltungsblätter, pp. 201 et seq. (at p. 203); Response of the Parliamentary State Secretary *Lintner* of

At the beginning of the 1990s, the triumphant rise of the Internet was accompanied by an exchange of illegal and harmful material which was intensively monitored by the press and public. Today the centre of attention is focused especially on child pornography, hate speech and libel in international computer networks.[78]

The distribution of child pornography and contents glorifying violence within the Internet and similar computer networks was illustrated in the famous "CompuServe-Case": In 1997, Bavarian State prosecutors indicted the head of the German CompuServe GmbH subsidiary for not having filtered pornographic newsgroups and games glorifying violence within the proprietary service, both types of data stored on servers of CompuServe Inc. in the USA.[79]

In 1996 the Spanish public was stunned by a case of distribution of child pornography. Two students had a collection of over 150 floppydisks with child pornography all collected over the Internet. Both had to be released from prison after 3 days because of a legal gap in the new Spanish Criminal Code of 1996.

Increasingly video games with a racial background in which the user could discriminate against foreigners and ethnic minorities served as propaganda material for young people. E.g., in the video game "Concentration Camp-Manager" – distributed mostly via BBS – the player must decide whether a foreign worker is first to be sent to work in a mine or whether he is to be gassed immediately.

An example for libel was dealt with by court in the United States in 1991.[80] In this case, CompuServe contracted with a third party for that user to conduct a special-interest forum (called "Rumorville") on CompuServe. The plaintiff claimed that defamatory material about its business was posted by a user in that forum, and sued both the forum host and CompuServe. CompuServe moved for, and received, summary judgement in its favour.[81]

The prosecution of perpetrators disseminating illegal contents in the Internet is not only made difficult by the fact that these perpetrators are acting from abroad and that the international mechanisms of co-operation are often weak and slow. Prosecution is often impossible since perpetrators can hide behind the *anonymity* which today is granted by anonymous remailers and by the abuse of free access software.

---

21 April 1994 to questions of the Member of Parliament *Böhm*, Bundestagsdrucksache 12/7357; "PC Computing", December 1989, pp. 146 et seq.; "Focus" No. 4/1995, pp. 52 et seq.; for the "Thule-Netz" cf. also "Chip" No. 3/1994, pp. 82 et seq.

78 With respect to copyright infringements on the Internet see supra chapter II.B.3.

79 For details of the case see *Sieber*, Strafrechtliche Verantwortlichkeit für den Datenverkehr in internationalen Computernetzen (1), (1996) Juristenzeitung, pp. 429 et seq.

80 The case was decided in the Southern District of New York, Cubby Inc. vs. CompuServe (776 F. Supp. 135, 1991).

81 See <http://www.eff.org/pub/CAF/law/libel_1.IW> (accessed on 22 January 1998).

Anonymous remailers are servers which delete the senders e-mail address or identity and replace it by a new identity given by the server. These anonymous remailers can be found in many countries.[82]

Another method to avoid the identification of perpetrators is the abuse of free access software. For example, if a user decides to subscribe to an online service like America Online (AOL) he can install the free access software and enter a fictitious name, address and bank account. Then the new subscriber is allowed to use the online service several (normally 10 to 30) hours for free. After that period a regular fee has to be paid (either time-depending or flat rate). However, neither the name and address nor the bank account is checked for its correctness. Therefore, it is no problem to use a faked name or the bank account of another person for a considerable period of time.

As a consequence, in many countries police forces and state prosecutors tried to force Internet access and service providers to erase or to block illegal contents. A technical analysis of the respective questions by the author of this report in 1997 shows that it is only possible to erase illegal data clearly defined on an own server. However, it is difficult to detect all illegal data on own servers and it is not possible to block access to other servers without severely damaging the advantages of international computer networks.[83]

The difficulties of blocking access to other servers were clearly illustrated when the German General Federal State prosecutor required several German providers to block access to the web server of the Dutch service provider "xs4all" which hosted the WWW pages of the periodical "radikal" containing illegal contents on how to sabotage railways. This request was followed by several German service providers. As a result numerous messages in various forms were broadcast on the Internet with information on new, alternative possibilities of accessing the page. E.g. one message hinted that "radikal" was now accessible under 36 new Internet addresses all over the world. Additional opportunities were offered to call up or order the periodical "radikal" via FTP service or e-mail. Finally, 25 different telephone numbers in the Netherlands were given, where users could directly log in with the identifier name "new", and, without an access to a provider, could download the periodical. The distinguished German Research Network, DFN, which is responsible for connecting the German university networks to the Internet, and which first suspended the address of "xs4all" at the request of the German Federal Prosecutor, therefore lifted the suspension at the end of April 1997. The reason the press officer of the DFN association gave for this fact was that the alternative dissemination of the suspended web-pages had proved that individual pieces of information could not be suspended.

82 A whole list of remailers can be found at <http://www.cs.berkeley.edu/~raph/remailer-list.html>, for more info on remailers see <http://anon.efga.org/anon/> (both accessed on on 22 January 1998).

83 See *Sieber*, Kontrollmöglichkeiten zur Verhinderung rechtswidriger Inhalte in Computernetzen, (1997) Computer und Recht, pp. 581 et seq., pp. 653 et seq.

D. Other Offences

Along with the advance of information technology to new areas of live computers can be (ab)used for almost all offences. This includes, e.g., threats to human life, various activities of organised crime as well as electronic warfare.

1. Attacks on Life

Computer manipulations described above did not only serve the purpose of gaining pecuniary benefits, but were also used for attacks on life – as in the case of the manipulation of a flight control system or of a hospital computer.

> An example for the spreading of computer crime in traditional fields of offences is the manipulation of a British hacker, whoaccessed the information system of a Liverpool hospital in 1994 because he simply wanted to see "what kind of chaos could be caused by penetrating the hospital computer". Among other things, he changed the medical prescriptions for the patients: A nine-year-old patient who was "prescribed" a highly toxic mixture survived only because a nurse re-checked his prescription.[84]

2. Organised Crime

It is obvious that the powerful tools of modern computer and communication systems to store, administer and transfer data are also used by organised crime groups in many areas. Organised crime[85] is especially involved in the above described acts of sophisticated computer fraud, credit card fraud, telephone fraud as well as software and product piracy. Computer data stored and transmitted in encrypted form is also used e.g. by drug and arms dealers to administer their activities. In the future, electronic money transactions and "cyber money" will be increasingly used for illegal gambling and for money laundering on the Internet.

> The involvement of organised crime groups in the field of computer fraud was illustrated when a Russian group attacked one of the best known US banks in New York via data networks in 1994. Operating from St. Petersburg, the group succeeded in causing the American bank to transfer over US$ 10 million to foreign accounts.[86] Monitoring and following the "money trail" of the manipulations, some of the perpetrators finally could be arrested. The responsible security officer of the bank told

84 Cf. for this case "Der Spiegel" No. 9/1994 of 28 February 1994, p. 243.

85 For the term and the various forms of "organised crime" see *Sieber/Bögel*, Logistik der Organisierten Kriminalität, 1993, pp. 23 et seq.

86 Cf. for this (1995) Datenschutz-Berater, Volume 10, p. 23.

the author that the arrested perpetrators possessed false Greek and Israeli passports which were forged in a quality which could be produced in Russia only by members of the former Russian secret service KGB.

3. Electronic Warfare

In the meantime, the possibilities of computer manipulations have also been recognised in the military sector. "Strategic Information Warfare" has become a form of potential warfare of its own.[87] This type of warfare is primarily directed to paralyse or manipulate the adversary's computer systems.

The dependency of military systems on modern information systems became evident in 1995 when a "tiger-team" of the US Air Force succeeded in sending seven ships of the US Navy to a wrong destination due to manipulations via computer networks.

There is no need to point out the possible danger originating from a manipulated nuclear power station in order to stress that meanwhile, computer misuse has become a global threat and the security of modern computer systems has gained central significance for the information society of our days.

E. Conclusions

Summing up the previous development and especially the recent changes of computer crime, the introductory notion of an accelerated adaptation of crime to information technology is confirmed. Considering the present development of computer crime and taking a look at future developments, four points must be emphasised:

1. Today, computer and telecommunication technology have spread into nearly all areas of life. Thus new computer crimes have become possible. In the future, this development will go even further: The Internet is becoming an "information superhighway" where pieces of music and movies can be retrieved by private homes and electronic commerce will play an important role. Defence systems, nuclear power stations, traffic control systems and other control systems are increasingly being shaped by computer

87 Cf. *Arquila/Ronfeldt*, Cyberwar is Coming!, Comparative Strategy, Volume 12 (1993), pp. 141 et seq.; *Molander/Riddile/Wilson*, Strategic Information Warfare – A New Form of War, 1996 (edited by the National Defense Research Institute RAND, Santa Monica/Ca).

technology as well. The information society will thus depend even more on information technology.

Thus, computer crime has become more frequent, more diverse and more dangerous.

2. The computer of the 1950s and 1960s was still an exclusive "device of power" in the hands of the state or of particular enterprises. Today it has become available for every citizen because of the increase in performance and the corresponding price drop of personal computers. This led to changes concerning computer offences both on the side of the criminals as well as victims.

As a consequence, computer crimes can nowadays be committed by nearly everybody and threaten – just as the other dangers of the "risk society" – every citizen.

3. Electronic data processing – as a consequence of a permanent "miniaturisation" of its components – is converging with telecommunications. Computer crimes are increasingly committed via telecommunication networks – also from abroad. New patterns of committing offences have developed, such as, e.g., telephone misuse, communication offences or manipulations via the Internet.

Thus, computer crime has become more mobile and more international.

4. Modern computer and communication networks have developed some specific characteristics which are especially useful for criminal perpetrators and very difficult to overcome for prosecutors: First, international computer networks (with anonymous remailers or free access devices to Internet service providers) offer anonymity to perpetrators which can only be lifted if all countries co-operate that are crossed by the communication.88 Second, computer and communication systems are increasingly offered together with strong encryption and possibilities to hide data. Today standard software is able not only to encrypt data but also to hide data e.g. in pictures (steganography). Thus, controlling data storage and data transmission has become much more difficult for prosecuting agencies.

88 This means, that as long as there are countries which do not co-operate, anybody wishing to hinder the lifting of his/her anonymity, merely has to provide for routing through one of these countries.

Thus, computer crime and the Internet have become especially attractive for organised crime groups.

Because of this development, the security of computer systems and the prevention of computer misuse have become the central questions of today's information society. The following third part of this report analyses how the law – and criminal law in particular – has taken up this challenge and how it has adapted to meet the latest developments.

III. National Law

As illustrated in the introduction, the adaptation of law to new forms of computer crime resulted in a multitude of different legal questions which can be traced back to six main waves of computer crime legislation: Protection of privacy (infra A), protection of economic criminal law (infra B), protection of intellectual property (infra C), protection against illegal and harmful contents (infra D), criminal procedural law (infra E) as well as legal regulations on security measures (infra F). The following analysis will differentiate between these main fields of computer-related law.

A. Protection of Privacy

1. Development and Mechanism of Privacy Protection

Contrary to the legal rules on corporeal objects, information law must only consider the economic interests of the proprietor or holder f information, but must also take into account the interests of those persons who are concerned by the content of information. Before the invention of computers, the legal protection of those persons was connected with criminal provisions on libel and traditional secrecy protection (e.g., in the medical field). However, these traditional provisions for the protection of personal honour and private secrets only covered part of the personality right and proved to be far too narrow for a protection against the new possibilities of collecting, storing, accessing, comparing, selecting, linking and transmitting data by new technologies. These new threats to privacy prompted many countries to enact, since the 1970s, new bodies of administrative, civil and penal regulations not only in general "horizontal" privacy laws but also in specialised "sectorial" legislation.

As a consequence of this historical development, a differentiation in criminal data protection law can be found in all countries: Traditional offences for the protection of secrecy (e.g. for physicians, lawyers or public officials) can still be found in the core of criminal law, i.e. in the various criminal codes. The general data protection laws – caused by the use of computers – contain criminal provisions that at first merely referred to

electronically stored data, but which have increasingly been extended to manually processed data in recent years as well. These general provisions are completed by data protection regulations for specific fields, which partly contain special criminal provisions, but which partly only refer to the criminal provisions in the general data protection laws. Furthermore, personal data obtain indirect criminal protection by general criminal provisions that are not limited to personal data.[89]

Since it is neither possible to compare all traditional provisions on libel and personal secrets nor the multitude of sectorial privacy laws,[90] the

89 Cf. especially for hacking and for economic espionage infra chapter III.B.1 and 2.

90 In Germany, e.g., the Statistics Act (Act on the Statistics for Federal Purposes of 22 January 1987, Bundesgesetzblatt I, p. 462), the 10th Book of the Social Security Code (10th Book of the Social Security Code of 18 September 1980, Bundesgesetzblatt I, p. 1469; last amended by the Justizmitteilungsgesetz of 26 July 1997, Bundesgesetzblatt I, p. 1430) and the Framework Registration Act of 1980 (Framework Registration Act of 16 August 1980, Bundesgesetzblatt I, p. 1429), the new Population Census Act of 1987 (Act on a Census of Population, Professions, Buildings, Housing and Workplaces (Population Census Act) of 8 November 1985, Bundesgesetzblatt I, p. 2078), since 1989 several new Police Acts of the states (cf. the First Draft for an Amendment of the Model Draft of a Uniform Police Act of the Federation and the Regions of 12 March 1986, Sections 8a-d, printed in *Kniesel/Vahle*, Vorentwurf zur Änderung des Musterentwurfs eines einheitlichen Polizeigesetzes des Bundes und der Länder, 1990, pp. 4 et seq. Cf. also, e.g., Saarland Police Act of 8 November 1989, Amtsblatt des Saarlandes, p. 1750 (Sections 25-40) or the Act about the Functions and Competences of the Bavarian State Police of 14 September 1990, Bayerisches Gesetz- und Verordnungsblatt, p. 397 (Articles 30-49)), in 1990 the Act Concerning the Federal Agency for the Protection of the Constitution and other Laws on the Secret Services (cf. Act on the Co-operation of the Federation and the States in Matters of the Protection of the Constitution and through the Federal Agency for the Protection of the Constitution (Act on the Federal Agency for the Protection of the Constitution) of 20 December 1990, Bundesgesetzblatt I, p. 2954), in 1991 the Data Protection Regulation on Postal Services, Postal Bank Services and Telecommunications (Regulation about the Data Protection in Services of the German Mail Postal Service/Postal Bank/Telecommunications of 24 June 1991, Bundesgesetzblatt I, pp. 1385, 1387, 1390) as well as – also in 1991 – the Act Concerning the Documents of the Former East German State Security Service (STASI) (Act Concerning the Documents of the State Security Service of the Former GDR of 20 December 1991, Bundesgesetzblatt I, p. 2272), the Act Against Illegal Drug Trafficking and Other Forms of Organised Crime of 1992 (Act Against Illegal Drug Trafficking and Other Forms of Organised Crime of 15 July 1992, Bundesgesetzblatt I, p. 1302. Regulations on data protection are in particular contained in Sections 98a, 98b, 98c of the Criminal Procedure Code, which were newly introduced by this law), the Money Laundering Act of 1993 (Act on the Tracing of Financial Benefits from Serious Crime – Money Laundering Act of 25 October 1993, Bundesgesetzblatt I, p. 1770), the Crime Prevention Act of 1994 (Act for the Amendment of the Criminal Code, the Criminal Procedural Code and Other Laws (Crime Prevention Act) of 28 October 1994, Bundesgesetzblatt I, p. 3186. Especially Sections 474 et seq. of the Criminal Procedural Code which have been amended by this law contain regulations about data protection. See also the Draft of a Criminal Procedural Code Amendment Act of 1996 (Bundesratsdrucksache 961/96 of 20 December 1996) and the new Telecommunications Act of 1996 (Telecommunications Act of 25 July 1996, Bundesgesetzblatt I, p. 1120) also contain specific data protection regulations. The

following comparative analysis concentrates on the general privacy laws. Since the penal provisions in these laws largely refer to the corresponding administrative provisions, it is necessary to begin by briefly surveying the administrative provisions and then to deal with the respective criminal law questions.

2. Differing Concepts of Data Protection Laws

Special legislation against infringements of privacy has been adopted in most Western legal systems with data protection laws of more or less general character.[91] Moreover, the courts in most countries developed a tort of privacy. An analysis of the national acts and bills shows that various international actions[92] have already achieved a considerable uniformity in the general administrative and civil law regulations of the national privacy laws. Most of the national data protection acts mentioned above[93] include, for example, provisions that cover the limitation of data collection or the individual's right of access to his or her personal data. In spite of this tendency, considerable differences in general administrative and civil regulations cannot be denied. These differences concern the legislative rationale, the scope of application (especially with regard to legal persons and manually recorded data), the procedural requirements for starting the processing of personal data, the substantive requirements for processing personal data, as well as the respective control institutions.

The differences among the general administrative regulations are not only relevant for administrative law, but to a large extent also determine differences of criminal law provisions which largely refer to these regulations. Consequently, one difference among the criminal offences in the national privacy laws concerns the various data the use of which is prohibited: On the one hand, legal systems which only have privacy regulations in specific areas, which only cover data linked to the name of individuals or which only apply in cases of automatic data processing generally have penal provisions with a more limited scope of application

---

Census Decision of the Federal Constitutional Court of 1983 (Entscheidungen des Bundesverfassungsgerichts, Volume 65, pp. 1 et seq.) contributed more than anything else to this development, because it stated that any interference with the citizen's right to informational self-determination (which was for the first time acknowledged by the decision) required an explicit legal basis.

91 For references see supra chapter I, fn. 17.

92 See infra IV.A.

93 See supra chapter I, fn. 17.

than, on the other hand, legal systems with comprehensive privacy legislation which includes data of legal persons and manually recorded data.

3. Differing Acts Covered by Criminal Law

The main differences among the penal privacy offences, however, do not lie in their general scope of application, but in the different illegal acts they cover. These differences in penal coverage are mainly caused by a divergent evaluation of the criminal character of privacy infringements and the role that penal law should play in this field: In some countries, especially in North America and Japan, criminal law is not widely used for privacy protection. This is the case in the United States legislation (which only contains a few penal provisions), in the Canadian privacy legislation (which only punishes the act of obstructing the work of the Information Commissioner and the Privacy Commissioner with an administrative fine), in the Japanese Personal Information Protection Law (which only covers the obtaining of personal information by an administrative fine), but also in the Data Protection Act of the Netherlands (which only punished the infringement of provisions on the registration of data files.[94] On the other hand, many European privacy laws include comprehensive lists of severe criminal offences which refer to many of the acts prohibited by administrative law. In France, the importance of criminal sanctions in privacy legislation has been stressed by including the most important infringements in the general Penal Code.[95]

The most important differences between the "crimes against privacy" in the various data protection laws become clear while analysing the penal provisions in detail. Such a comparative analysis must distinguish four main categories of criminal privacy infringements which can in particular be found in the European privacy laws: infringements of substantive privacy rights (infra a), infringements against formal legal requirements (infra b), infringements of access rights (infra c), and neglect of security measures (infra d).

a. Infringements of Substantive Privacy Rights

The first main group of "crimes against privacy" is constituted by infringements of substantive privacy rights and includes the following acts:

94 See the references supra chapter I, fn. 17.

95 See Article 226-16 – Article 226-24 Nouveau Code Pénal.

- the illegal disclosure, dissemination, obtainment of and/or access to data, acts which are covered in most laws, however, to different extents
- the unlawful use of data, which is a criminal offence only in a few countries
- the illegal entering, modification, and/or falsification of data with the intent to cause damage, an act which is criminalised in the privacy laws and in the general statutes of the criminal law of some countries
- the collection, recording, and/or storage of data which is illegal for substantive reasons, acts which are criminalised only in a few privacy laws
- the storage of incorrect data, an act which in most countries is covered by the general offences of information and in some countries by additional statutes within the privacy laws.[96]

A detailed analysis of the respective criminal provisions shows that these substantive infringements of privacy rights not only differ in the data covered and in the types of acts punished. They differ further according to the extent to which the described acts are permitted by law. Since the penal provisions either refer to the respective general provisions of the privacy laws or regulate the justification of the use of personal data by general clauses which are similar to those of the administrative provisions, all heterogeneities, inaccuracies and uncertainties in the field of administrative law can also be found within the respective penal provisions.[97]

b. Infringements Against Formal Requirements

As a result of the uncertainties of the substantive provisions, many legal systems rely to a great extent on a second and additional group of offences against formal legal requirements or orders of supervisory agencies. This

96 Most of the respective provisions are contained in the general data protection acts cited supra chapter I, fn. 17. See, for Austria, Sections 48 and 49 Data Protection Act; for Denmark, Section 27 (1) No. 1 Private Registers Act and Section 29 (1) No. 1 Public Authorities' Registers Act; for Germany, Section 203 Penal Code and Section 43 Federal Data Protection Act of 1990; for Finland, Section 45 of the Personal Registers Act 1987; for France, Sections 41, 42, 43 and 44 Data Protection Act; for Israel, Sections 2 (5), (9); 16; 23B of the Protection of Privacy Law; for Italy, Article 35 Data Protection Law; for Luxembourg, Articles 33, 34, 35 of the Act Regulating the Use of Nominal Data; for Sweden, Sections 20 (3), (4); 21 of the Data Protection Act; for the UK, Section 15 of the Data Protection Act; for the USA, the Fair Credit Reporting Act 1970 (codified, as amended, at 15 U.S.C. §§ 1681-1681t), the Privacy Act 1974 (codified, as amended, at 5 U.S.C. § 552a), the Cable Policy Act of 1984, the Electronic Communications Privacy Act of 1986 (codified at 18 U.S.C. §§ 1367, 2232, 2510-2522, 2702-2711, 3117, 3121-3127), and the Video Privacy Protection Act of 1988 (codified at 22 U.S.C. § 2000aa) as well as various state laws (see for an overview on State Data Protection Laws in the United States *Perritt*, Law and the Information Superhighway, 1996, pp. 115 et seq.).

97 See, for Germany, *Haft*, Zur Situation des Datenschutzstrafrechts, (1979) Neue Juristische Wochenschrift, pp. 1194 et seq.; *Tiedemann*, Datenübermittlung als Straftatbestand, (1981) Neue Juristische Wochenschrift, pp. 945 et seq.

change from a substantial to a procedural approach was supported by a widespread opinion in Europe that data protection laws should not only prevent abuses in the field of privacy, but also provide a general scheme determining the circulation of information in society.[98] The formal offences against supervisory agencies and regulations which are, furthermore, included in most privacy laws contain in general more precise descriptions of the prohibited acts than of the substantive offences. However, these formal provisions also vary considerably within the national legislation.

The differences among the formal offences are not only based on differences in administrative law concerning the existence, nature, and powers of supervisory agencies, and the respective duties of the data processors. Mainly they are evoked by different answers to the fundamental question whether "formal" offences should be regarded as criminal or not. This leads to the fact that some countries, such as Denmark or France, punish formal offences against supervisory agencies and regulations with severe criminal sanctions, while others, such as Germany, regard such offences as "Ordnungswidrigkeiten", "petty offences" or "administrative offences", only punishable by fines. In the Italian Data Protection Act, it is a criminal offence not to comply with the decrees of the Supervisory Authority, and it is an administrative offence not to provide the Supervisory Authority with the necessary information or documents. Likewise the formal offences criminalised vary among the various privacy laws: the main type of formal infraction covered in many states by penal law concerns the infringement of the legal requirements for starting personal data processing (registration, notification, application for registration, declaration, or licensing). Additional – and considerably varying – formal offences which can be found in many European privacy legislations are: the infringement of certain regulations, prohibitions, or decisions of the surveillance authorities; the refusal to give information or the release of false information to the surveillance authorities; the hindering of the surveillance authorities; the refusal to grant access to property and the refusal to permit inspections by surveillance authorities; the obstruction of the execution of a warrant; the failure to appoint a controller of data protection in the company, as well as

98 See, for example, *Simitis*, Data protection – A few critical remarks, in: Council of Europe/Camera dei Deputati (eds.), Legislation and Data Protection – Proceedings of the Rome Conference on Problems Relating to the Development and Application of Legislation on Data Protection, 1983, pp. 171 et seq.

neglecting to record the grounds or means for the dissemination of personal data.[99]

c. Infringements of Access Rights

A third type of criminal privacy infringement is the infringement of access rights (the individual's rights of information or freedom of information). With regard to a party's right of access, in many European countries – such as in Denmark, Luxembourg and Sweden – it is an offence to give false information, not to inform the registered party or not to reply to a request. According to German law, this act is considered to be an "Ordnungswidrigkeit" which is punishable by a fine.[100] A non-criminal comprehensive system providing access to government information can be found especially in the USA.[101]

d. Neglect of Security Measures

Some countries even go further and punish the neglect of security measures with an administrative fine or even with a criminal sanction – the fourth type of offence. This is the case in the Luxembourgian, the Danish and the Italian privacy acts.[102]

---

99 Most of the respective provisions are contained in the general data protection acts cited supra chapter I, fn. 17. See, for Austria, Section 50 (1) of the Data Protection Act; for Denmark, Section 27 (1) No. 1 and 2, Section 27 (2) No. 4 Private Register Act; for Germany, Section 44 of the Federal Data Protection Act of 1990; for France, Sections 41 and 42 of the Act on Data Processing, Data Files, and Individual Liberties; for Italy, Sections 34-39 of the Data Protection Act; for Luxembourg, Sections 32, 37 of the Act Regulating the Use of Nominal Data; for Sweden, Section 20 (1), (2), (6) Data Act; for the UK, Sections 5 (5); 6 (6); 10 (9); 12 (10) of the Data Protection Act; for the USA, Section 522a para. i (2) of the Privacy Act 1984.

100 Most of the respective provisions are contained in the general data protection acts cited supra chapter I, fn. 17. See, e.g., for Denmark, Section 27 (1) No. 1 of the Private Registers Act; for Germany, Section 44 (1) No. 3 of the Federal Data Protection Act of 1990; for Luxembourg, Section 34 of the Act Regulating the Use of Nominal Data; for Sweden, Section 20 (5) Data Act.

101 See, for the USA, the Freedom of Information Act 5 U.S.C. § 552.

102 Most of the respective provisions are contained in the general data protection acts cited supra chapter III, fn. 17. See, for Denmark, Section 27 (1) No. 2 Private Registers Act; for France, Section 42 Act on Data Protection, Data Files and Individual Liberties; for Luxembourg, Section 36 of the Act Regulating the Use of Nominal Data. For Italy, Article 36 Data Protection Act, Article 36 (2) of the new Italian Data Protection Act punishes the unpremeditated failure to adopt appropriate data security measures.

4. Comparative Analysis

The analysis of the still existing differences between the national legal systems shows – in particular in criminal law – an important difference between the European and the Anglo-American data protection laws: Whereas Anglo-American law uses criminal provisions only reluctantly, European data protection laws also impose an accessory criminal sanction on most violations of provisions of purely civil and administrative nature. The classic ultima-ratio-function of criminal law and the requirements of certainty for blanket criminal provisions are strong arguments against the European concept. Europe therefore needs a decriminalisation which concentrates criminal law to clearly determinable and grave violations of data protection.[103]

B. Economic Criminal Law

The second reform wave of computer-specific legislation developed at the beginning of the 1980s as a reaction to computer-related economic crime. Legal amendments became necessary because new forms of computer crime posed a threat not only to the traditional objects of criminal law protection, but also to intangible goods (e.g. bank deposit money or computer programs). These new forms of computer crime also meant by new ways of committing traditional offences (e.g. computer manipulations instead of deceiving a human). In order to avoid an extension of the wording of already existing offences, many countries passed new laws for the fight against computer-specific economic crime and also provided for new offences for the prevention of unauthorised access to computer systems.[104]

At the beginning of the 1980s these new laws concentrated on computer-related economic fraud; further legislation concerned sabotage, espionage and illegal access. However, when these acts were increasingly committed via telecommunication systems from outside the entity maintaining the computer system at the end of the 1980s, it was realised in many countries that a basic "hacking" provision against such illegal access to computer systems is a fundamental requirement for the effective prevention of all economic crimes and moreover of all types of computer

103 For parallel developments on the international level see infra chapter IV.A.2.

104 For references see supra I, fn. 19.

crime. As a consequence, an effective protection against mere illegal access to computer systems ("hacking") plays a dominant role today not only in the field of economic criminal law, but also in general. For that reason the following analysis starts with discussing the basic hacking offence. It will then deal with computer espionage, software and other forms of product piracy, computer sabotage and computer extortion as well as computer fraud.

1. Hacking and/or Illegal Use as "Basic Offences"

Before the invention of computers, the exclusive access to specific private data was already covered by criminal law provisions concerning the secrecy of correspondence, the secrecy of telephone communication and for material within the scope of professional secrecy. The importance of private, economic and political information, stored in or transmitted by computers, then required the extension of such a "formal sphere of secrecy" at least to certain computer-stored data. The legal protection of specific computer-stored data can also be regarded as a new analogy in the information society to age-old notions of breaking, entering and trespassing.[105]

However, in most countries, a protection of this "formal sphere of secrecy" against illegal access to computer-stored data and computer communication could not be guaranteed by traditional criminal provisions. As far as wiretapping and the interception of data communications are concerned, the traditional wiretap statutes of most legal systems only refer to the interception of oral communication, as illustrated by the traditional wiretap statutes of Germany, Italy, the Netherlands and the United States.[106] Similarly, the provisions on trespassing and forgery cannot be used.[107] In all countries, the applicability of penal provisions is even more difficult with respect to unauthorised access to data processing and storage systems.

In response to the new cases of "hacking", many states developed new statutes protecting a "formal sphere of secrecy" for computer data by

105 For more details concerning the justification of the new "access" provisions, see *Sieber*, Informationstechnologie und Strafrechtsreform, 1985, pp. 51 et seq. Arguments against an "access provision" are stressed by *Kaspersen*, Strafbaarstelling van computer mis-bruik, 1990, pp. 346 et seq.

106 See, e.g., for Germany, Section 201 Penal Code; for Italy, Section 617bis, 623bis Penal Code; for the USA, 18 U.S.C. §§ Sections 2510-2521, 47 U.S.C. § 605. Similar problems arose under Canadian law with respect to Sections 183 et seq. Criminal Code.

107 See, for the UK, *R. v. Golf and Shifreen*, (1988) AC, wp. 1063.

criminalising the illegal access to or use of a third person's computer or computer data.[108] Legislation covering wiretapping and unauthorised access to data processing and communication systems[109] have, therefore, been enacted in Australia, Canada, Denmark, Germany, Finland, France, Luxembourg, the Netherlands, Norway, Spain, Sweden, Switzerland, the United Kingdom and the United States.[110]

On the other hand, however, there are still some countries – such as Belgium, Japan and Austria[111] – that do not have special criminal law provisions against hacking (i.e. the mere penetration into foreign computer systems). A corresponding criminal offence would be desirable in accordance with existing international recommendations.[112]

Moreover, the new laws which have been enacted or proposed demonstrate various approaches, which range from provisions criminalising "mere" access to DP-systems (Australia, Denmark, England, Greece and the

---

108 This concept of protecting a "formal sphere of secrecy" (or guaranteeing a "pax computationis") is not in contradiction with the concept of "freedom of information", because it is limited to specific data stored in a private computer.

109 Legal provisions defining the term computer in most countries resort to technical definitions which often suffer from overbreadth (including e.g. handheld calculators, new kitchen stoves and electronic typewriters). These problems are avoided in a 1983 Tennessee statute which defines "computer" in terms of function as "a device that can perform substantial computation, including numerous arithmetic or logic operations, without intervention by a human operator during the processing of a job. See Tennessee Code An. Section 39-3-1403 (2) (Supp. 1988).

110 See for Canada, Article 342.1 Criminal Code (using the slightly wider concept of "interception" as opposed to "access"); for Denmark, Section 263 (2) and (3) Penal Code, for Germany Section 202a Penal Code; for Finland, chapter 38 Section 8 of the Penal Code (as amended 1990); for France, Article 462-2 Criminal Code, amended in 1988; for Greece, Article 370 C (2) Criminal Code, as amended in 1988; for Luxembourg, Article 509-1 Penal Code, as amended in 1993; for the Netherlands, Article 138a (1), (2) Criminal Code, amended 1992; for Norway, Section 145 Penal Code, amended 1987; for Spain, Article 256 Criminal Code 1995; for Sweden, Section 21 Data Protection Act; for the UK, Sections 1, 2 Computer Misuse Act 1990; for Switzerland, Article 143bis Criminal Code; for the USA, the Electronic Communications Privacy Act of 1986 (18 U.S.C. §§ 2510-2521, 2701-2710, 3117, 3121-3126), the Computer Fraud and Abuse Act of 1984 and 1986 (codified at 18 U.S.C. §§ 1029, 1030) as well as various state laws.

111 In Austria, mere hacking could only be punished – according to the respective circumstances – under the aspects of data protection (Section 49 Data Protection Act) and alteration of data (Section 126a Criminal Code) or at least attempt thereof, cf. *Schick/Schmölzer*, in: Sieber (ed.), Information Technology Crime, 1994, pp. 26 et seq. In Japan, hacking is, also after the criminal law reform of 1987, only punishable with regard to certain consequences of the offence, e.g. as obstruction of business (Article 234-2 Penal Code) or theft of electricity (Article 245, 235 Penal Code); cf. *Yamaguchi*, in: Sieber (ed.), Information Technology Crime, 1994, pp. 314 et seq.

112 Apart from that, the use of abstract strict-liability offences for the prevention of computer viruses is increasingly being called for; cf. e.g. for Japan *Yamaguchi*, in: Sieber (ed.), Information Technology Crime, 1994, p. 316.

majority of states of the USA), to those punishing access only in cases where the accessed data are protected by security measures (Germany, the Netherlands, Norway), where the perpetrator has harmful intentions (Canada, France, Israel, New Zealand, Scotland), where information is obtained, modified or damaged (some states of the USA) or where a minimum damage is caused (Spain). Some countries (e.g., Finland, the Netherlands, the United Kingdom) combine several of these approaches in one or more provisions with a "basic" hacking offence and the creation of qualified forms of access (in a more serious "ulterior" offence) carrying more severe sanctions. A wide range of criminal law protection exists, e.g., in the new English law which enacted three new "hacking offences" covering in a "basic" offence, a person "if he causes a computer to perform any function with the intent to secure access to any program or data held in any computer". A few laws in the USA go even further and criminalise preparatory acts such as "password swapping",[113] whereas other countries rely in this respect more on the general rules of inciting, counselling and procuring the offence. On the other hand, some scholars suggest giving a certain "premium" for cases in which the perpetrator immediately indicates the unauthorised access to the victim or to public authorities.[114]

A specific discussion concerns the circumstances under which initially authorised access may become unauthorised or may otherwise turn into a criminal action. In most countries the new provisions only deal with initially unauthorised access (thus only criminalising acts of outsiders), whereas other countries also cover illegal staying in systems (thus also covering time theft by employees).[115] A special solution can be found in the California State Law which does not apply to employees if their use is within the scope of their employment or (for uses outside the scope of employment) if the use does not result in an injury or if the value of the used services does not exceed US$ 100.[116]

The discussion about initially authorised access shows that the illegal access to computer systems is closely connected and partly overlaps with

113 In the USA Title 18 Section 1030 (a) (6) of the United States Code criminalises "whoever ... knowingly and with intent to defraud traffics ... in any password or similar information through which a computer may be accessed without authorisation." Californian Law penalises one who "knowingly and without permission provides or assists in providing a means of accessing a computer"; see Californian Penal Code Section 502 (c) (6). See also for Canada supra chapter I, fn. 21.

114 See *Sieber*, The International Handbook on Computer Crime, 1986, p. 90.

115 Arguments against an extension of criminal law in this area are, that it would punish acts such as walking into another person's office or entering a building somewhat later than usual.

116 See Section 502 (h) (2) California Penal Code.

the criminalisation of unauthorised use of computers ("time theft"), though up to the present this close relationship has not yet been generally realised. *De lege ferenda*,[117] in most European countries the problem of illegal use of computers is reduced to the illegal use of computer hardware and discussed within the context of *furtum usus* of corporeal property. In this context many European countries, such as Germany, France, Greece or the United Kingdom, as well as Israel, reject a general criminalisation of *furtum usus* of tangibles (with exceptions especially for motor vehicle joyriding) and consequently did not incorporate a provision against illegal use of computers or "time theft" in their new computer crime laws.[118] On the other hand, there are (mainly Nordic) countries which have a tradition covering illegal use of corporeal property,[119] and consequently the Swedish, Finnish and Norwegian laws criminalise the unauthorised use of tangible property including computer systems.[120] A different approach in enacting special statutes which only cover the unauthorised use of computers was followed in Canada, the Netherlands and the United States of America.[121]

In general, the discussion on "time theft" does not distinguish sufficiently between the illegal use of computer hardware and the illegal use of computer data, just as the interaction between illegal access and illegal use of computer data is not sufficiently considered. Since illegal use of data generally presupposes illegal access to data, an adequate "access provision" could at the same time cover illegal use of data. On the other hand, an additional criminal provision covering the illegal use would include the above-mentioned acts of insiders. Consequently, the new "criminal information law" should only contain one access-and-use-provision which is restricted to computer-stored data and especially deals with the problem of initially authorised access becoming unauthorised. As future technical

---

117 De lege lata, in most countries the unauthorised use of computer services or "time theft" is not covered by the traditional penal provisions on theft, breach of trust, unauthorised use of another person's property, unauthorised use of automatic vending machines or public telephone networks as well as unlawful use, waste, or withdrawal of energy. For details see *Sieber*, The International Handbook on Computer Crime, 1986, pp. 81 et seq.

118 This solution is consequent only with respect to the use of computer hardware and not with respect to the use of computer software; see infra.

119 See, e.g., for Belgium, Section 461 Penal Code; for Denmark, Section 293 Penal Code; for Finland, chapter 28 Sections 7-10 of the Penal Code (as amended 1990).

120 See, for Finland, chapter 28 Sections 7-10 of the Penal Code (as amended 1990); for Norway, Section 261 of the Penal Code, amended in 1986; for Sweden, chapter 8 Section 8 Criminal Code and chapter 10 Section 7 Criminal Code, as amended in 1986. See also for Switzerland, Article 150 Criminal Code.

121 See, for Canada, Section 342.1 (1) (a) Criminal Code; for the Netherlands, Article 138a (3) Criminal Code; for the USA, 18 U.S.C. § 1030 as well as various State laws.

developments will make it more and more difficult to distinguish between telecommunication systems and computer systems, it should also be considered to combine wiretapping and unauthorised access to computer systems in one provision.[122]

2. Computer Espionage

The historical and comparative analysis of trade secret protection is a perfect illustration for the theory that legal provisions, developed for tangible property, cannot easily be applied for the protection of information.

When information is acquired by taking away another person's corporeal information carrier (such as a printout, tape or disc), the traditional penal provisions on theft, larceny or embezzlement do not create special problems in all legal systems. However, the ability of data processing and communication systems to copy data quickly, inconspicuously and often via telecommunication facilities has replaced most of these traditional "information carrier thefts" with acts of copying information onto data storage devices. Therefore, the question arises as to what extent pure acquisition of incorporeal information can or should be covered by these provisions. Most continental law countries, such as Austria, Belgium, Germany, Greece and Italy, are reluctant to apply the traditional provisions on theft and embezzlement to the unauthorised "appropriation" of secret information, because these laws generally require that corporeal property is taken away with the intention of permanently depriving the victim of it.[123] However, in some continental law countries – such as France – the application of the traditional provisions on theft and embezzlement seems possible at least in certain cases.[124] In Japan, the definition of the intention of unlawful appropriation has been widened, and now includes the intent to use property only temporarily; nevertheless, Japanese law still requires the taking of tangible property and cannot be applied if data are accessed via telecommunication facilities.[125] A stronger tendency towards a "property theory" of intellectual values can be found in most of the common law countries, especially in Australia, the United States and – controversially discussed – in Canada. In the United States, for example, some courts

122 For the respective proposals of international organisations see infra chapter IV.B.

123 See, for Austria, Section 127 Criminal Code; for Belgium, Section 461 Penal Code; for Germany, Sections 242, 246 Penal Code; for Italy, Sections 624, 646 Penal Code.

124 See, for France, Section 379 Penal Code.

125 See for Japan, Article 235, 252, 253 Penal Code.

regarded computer data as property in the sense of traditional larceny provisions and in many states the legislatures have defined computer data or trade secrets as "property" or a "thing of value", to enable the application of the larceny provisions or new general provisions on computer crime. Canadian – and similarly Israeli – legislation which originally followed a property approach for information, changed to recognising that information per se cannot be the subject of taking away.[126]

Due to the above-mentioned differences in the nature of corporeal property and intellectual values (property implies exclusivity, while information tends to be conceived as a public good), the difference between traditional property rights and intellectual property rights (for example concerning the question of ownership and possession), as well as the difference between traditional theft of tangible things and the theft of information (in which the information in question is only copied and remains with the owner), a theory of property should be denied for the general protection of intellectual values.[127] One has to keep in mind that civil law does not regard information per se as protectable and that even with the statutory monopolies of copyrights, patents, trademarks and industrial designs, the creator, inventor or designer of the work is only given exclusive ownership rights within certain limits (especially with respect to time and geographic areas).

As a result of the problems in applying the general property law to cover trade secrets in most continental law countries, the misappropriation of someone else's secret information is covered by special provisions of trade secrets law. These provisions protect trade secrets by prohibiting certain condemnable acts of obtaining information, either by provisions of the penal code or by penal or civil provisions of acts against unfair competition.[128] Reform laws strengthening penal and civil trade secret protection have been enacted in recent years in Canada, Denmark, Germany, the Netherlands,

126 For a detailed analysis of the relevant court decisions of common law countries see *Sieber*, Legal Protection of Computer Data, Programs and Semiconductor Products – A Comparative Analysis with Suggestions for Legal Policy, in: International Chamber of Commerce (ed.), International Contracts for Sale of Information Services, 1988, pp. 7 et seq.

127 See *Hammond*, Quantum Physics, Econometric Models and Property Rights to Information, 27 (1981) McGill Law Journal, pp. 47 et seq.

128 See, for Austria, Sections 11, 12, 19 of the Act Against Unfair Competition and Sections 122-124 Criminal Code; for Germany, Sections 17, 18, 20 of the Act Against Unfair Competition; for Finland, chapter 30 Sections 4-6 of the Penal Code (as amended 1990); for France, Section 418 Criminal Code; for Italy, Section 623 Penal Code; for Spain, Articles 278, 279, 280 Criminal Code 1995.

Sweden, the United Kingdom and the United States.[129] This concept of trade secret protection and fair competition is in harmony with the modern American information theory which rejects the static "property-theory" and turns to procedural "relationship-theories" and "entitlement-theories" by looking at the relationship between discloser and disclosee.[130] However, generally speaking, it can be said that criminal trade secret law and civil unfair competition law are less developed in Anglo-American countries (especially in Canada, Israel and the United Kingdom), as well as in Asian countries (especially in Japan), than in continental Europe. In Japan, e.g., the amendments to the Unfair Competition Act enacted in 1990 did not include any penal sanctions.

As far as future policy making is concerned, the international trend towards trade secret protection should be encouraged. In order to achieve an international consensus it is recommended that all legal systems – either in their penal codes or in the acts against unfair competition – establish penal trade secret protection backed up by adequate civil provisions concerning unfair competition.[131] These penal and civil provisions should generally apply to all trade secrets and not be limited to the computer and data processing area. However, in order to avoid the monopolisation of information, trade secret protection should be restricted to certain intolerable acts of obtaining information, and not be extended to a protection of information per se.[132]

Similar principles guarantee the protection of other secrets and of confidentiality, especially the secrecy of public authority, professional secrecy (especially for medical doctors and lawyers), mail and telephone confidentiality, or tax secrecy. Since these legal provisions do not play a dominant role in the field of computer crime, they are not dealt with in detail here.

---

129 See, e.g., for Denmark, the qualifications in Section 263 and 264 Penal Code, amended in 1985; for Germany, Section 17 of the Act Against Unfair Competition, amended in 1986; for Sweden, Section 21 Data Protection Act, chapter 10 Section 5 Criminal Code, Protection of Trade Secrets Act 1990; for Switzerland, Article 143 Criminal Code; for the USA, The Economic Espionage Act of 1996 (18 U.S.C. §§ 1831-1839). For a very broad protection of computer stored data see Article 138a (2) of the Dutch Criminal Code.

130 See Institute of Law Research and Reform, University of Alberta, Background Paper on Improper Interference with Computers and the Misappropriation of Commercial Information, 1983, pp. 44 et seq.

131 For the relevant activities of international organisations see infra chapter IV.B.

132 See Institute of Law Research and Reform, University of Alberta, Protection of Trade Secrets, Report for Discussion No. 1, 1984.

3. Computer Sabotage

Not only with respect to the protection of the exclusive use of information, but also with regard to the protection of the integrity of information, criminal law has a fragmentary character and is generally only to be used as an *ultima ratio* means. It is therefore impossible to protect the integrity of information with a general criminal provision, such as corporeal property is protected by statutes on damage to property. However, in guaranteeing the *integrity of specific data*, criminal law can play an important role in providing a "formal sphere of integrity" similar to the above-mentioned "formal sphere of secrecy" guaranteed by the hacking provisions.

Until the 1980s, in most legal systems the integrity of computer-stored data was covered by general provisions for damage to property, vandalism or mischief. However, these provisions were developed to protect tangible objects, so that their application in the information sphere posed new questions. In a few criminal codes, such as in Belgium law or in Australian state law, the mere erasure of information without damaging the physical medium did not fall under the provisions of damage to property, since electric impulses are not considered to be "corporeal property" and interference with the use of the physical medium is not considered to be "destruction".[133] On the other hand, the prevailing opinion in most countries considers the deliberate damage or destruction of information on tapes or discs as damage to property or vandalism *de lege lata*.[134] This conclusion is justified by the argument that the perpetrator either damages or interferes with the function of the physical tape or disc upon which the information is stored. However, even in these countries, problems occur in cases in which data are not recorded on corporeal carriers but are just transmitted.

In order to clarify the situation, legislation has been enacted in Austria, Canada, Denmark, Germany, Finland, France, Japan, the Netherlands, Spain, Sweden, Switzerland, the United Kingdom and the United States.[135]

---

133 See, e.g., for Belgium, Sections 528, 559 Penal Code; for Canada, Sections 428, 430 Criminal Code.

134 See, e.g., for Austria, Section 125 Penal Code; for Denmark, Section 291 Penal Code; for Germany, Section 303 Penal Code; for Italy, Sections 420, 635 Penal Code (controversially disputed); for Japan, Articles 258-261 Penal Code and in addition Articles 233, 234 concerning obstruction of business; for the Netherlands, Section 350 Criminal Code; for Norway, Section 291 Penal Code; for Spain, Articles 547 et seq. of the old Criminal Code; for Sweden, chapter 12 Section 1 Criminal Code.

135 See for Austria, Section 126a Penal Code; for Canada, Section 430(1.1) Criminal Code; for Denmark, Section 193 Penal Code, amended in 1985; for Germany, Sections 303a and 303b Penal Code; for Finland, chapter 35 Sections 1-3, amended 1990, chapter 34 Section 1 para. 2 Penal Code, amended 1995; for France, Articles 462-3 and 462-4 Criminal Code; for Japan,

However, in these countries the statutes use different legislative techniques: Some countries (such as Finland) have the intention of amending the traditional statutes on mischief, vandalism or damage to tangible property, whereas, other countries create specific provisions for information. A few countries (especially Japan) cover all kinds of documents and not only computer-stored data. Others (Austria, Germany, France, Japan, the Netherlands, New Zealand, Spain, the United Kingdom) specifically protect the integrity of computer-stored data. Some legal systems also include specific qualifications for computer sabotage leading to the obstruction of business or of national security.[136]

Independent statutes which protect the integrity of computer stored data have the advantage that they can include the destruction or erasure of computerised data and their alteration or manipulation (a form of attack which is typical for information and not for tangible property), as well as the interference with the lawful use or access of data. Such comprehensive statutes can be found in Austria, Canada, Germany, Luxembourg and France.[137] These provisions are to be recommended as they protect a "formal sphere of integrity" for computerised data similar to the "formal sphere of secrecy" covered by the above-mentioned "access"-provisions.[138]

Whereas the majority of these new statutes on computer sabotage still require an actual damage of the victim and a respective intent of the perpetrator, some countries went even further by creating new independent provisions on the distribution and/or the production of viruses which partly or completely do not require these traditional requirements of vandalism or mischief. However, the extent to which the various national laws give up the traditional requirements of damage and intent varies: A "modest" extension of criminal liability was enacted in the UK by Section 3 of the "Computer Misuse Act 1990" according to which intent needs to be directed "at ... any particular computer, ... any particular program or data or a program or a data of any particular kind". This means that it does not have to be proved

---

Articles 234-2, 258, 259 Penal Code; for the Netherlands, Articles 350a, 350b Criminal Code; for Spain, Article 264.2 Criminal Code 1995; for Sweden, Section 21 Data Protection Act; for Switzerland, Article 144bis Criminal Code; for the UK, Section 3 Computer Misuse Act 1990; for the USA, Section 18 U.S.C. § 1030 (a) (5), as well as various state laws.

136 See, for Germany, Section 303b Penal Code; for Italy, Section 420 Penal Code; for Japan, Article 234-2 Penal Code; for Norway, Section 151b Penal Code.

137 See, e.g., for Luxembourg, Articles 509-2 and 509-3 Penal Code.

138 In the future, it should be carefully considered whether or not this formal protection of computerised data should be extended to other data (e.g., stored on paper). For the respective proposals of international organisations see infra chapter IV.B.

that the defendant had any specific computer or data as target in mind.[139] In the US, six states have passed further-reaching laws which specifically address the virus problems.[140] In most of these states, the extension is limited to criminal liability for the introduction or insertion of a "computer virus", a "destructive program" or a "computer contaminant". Minnesota and Nebraska have gone a step further by criminalising already those who "distribute without authorisation and with intent to damage or destroy any computer system or software or data". In Italy and in the Netherlands, an approach was taken similar to that of the US states just referred to: The new Italian law (Section 614 quinquies of the Criminal Code, introduced in December 1993) criminalises the introduction, communication or passing on of a data processing program which was the purpose or the effect of damaging a data processing or telecommunication system or its data or programs or of interrupting or altering its operation. The new Dutch provision covers "any person who intentionally or unlawfully makes available or distributes any data which is meant to do damage by replicating itself in an automated system, however, shall not be an offence to carry out the act ... with the object of limiting damage resulting from such data."[141] An even broader provision entered into force in Switzerland on 1 January 1995. There, not only the "production of a malicious program" is a crime, but also giving instructions to create such programs: "Anyone, who creates, imports, distributes, promotes, offers, makes available, circulates in any way, or gives instructions to create programs, that he/she knows or has to presume to be used for purposes according to item 1 listed above (to delete, modify or render useless without authorisation electronically or similarity stored or transmitted data), will be punished".[142]

---

139 Thus, Section 3 is held applicable e.g. to a case where the defendant intentionally introduced a computer "worm" program into a system, where it uses up all the spare capacity by adding programs or data thereby impairing the operation of the computer, if somebody intentionally introduces into circulation a disk contaminated with a "virus" and another person innocently uses it on his own computer, impairing its operation, this also is considered in the UK as an "unauthorised modification".

140 The six US states are California, Illinois, Maine, Minnesota, Nebraska, and Texas.

141 In a comment on this provision it is emphasised that the offender must have the intent to cause damage. The data will have to be suitable for that purpose; the intent could be proven by securing and analysing the virus. The term "multiplying" can also be understood to include simple copying as a first step. A person who tries to prevent damage and intentionally distributes and disposes anti-virus programs has a legal justification.

142 Similarly in 1992, a Swedish Commission came to the conclusion that as "computer viruses" could cause serious damage in a great number of computers through their propagation an additional offence should be introduced in the Criminal Code. The proposal included not only the case of "distribution " but also – like in Switzerland – that of "production". It reads as follows: "(1) Whoever creates a computer program or program instructions constructed in such a way that

However, it has to be noted that still most legislators who have introduced new computer crime laws or have amended them during the last ten years have not or not yet followed this line. The hesitation may come from the feeling that criminal law has only a limited effect in this field. Furthermore, it has not really been tested whether "traditional" provisions on computer sabotage could be sufficient for handling the problem. In many cases of distribution of viruses, a *dolus eventualis* of the perpetrator with respect to damage can be assumed.

4. Computer Forgery

One of the most important criminal law provisions covering the integrity as well as the correctness of specific information[143] are the provisions on forgery, which guarantee the authenticity of the author as authority for the statement which they contain.[144] In some countries, the traditional provisions on forgery require visual readability of the statements which are embodied in the document and, for this reason, do not cover electronically stored data.[145] With the intention of giving electronically based documents the same legal protection as paper based declarations, some countries – such as Australia, Canada, Germany, Finland, France, Greece, Japan, Luxembourg, the United Kingdom and Norway – enacted or proposed new statutes on forgery which relinquish visual perceptibility.[146] *De lege lata*,

---

they are capable of affecting data or the technical equipment used to process data without having authorisation to do so, or (2) spreads the aforementioned programs or instructions, and thus causes a risk of data being destroyed or altered, or causes damage to the aforementioned equipment or disturbance in its functioning, shall be judged guilty of manufacturing or spreading computer viruses, and sentenced to pay fines or to not more than two years of imprisonment." This proposal for an extension was accompanied by an extension of the required culpable state of mind which other legislators had not dared introducing up to now. Even if the offence had been committed by gross negligence, and not by intent, is should be possible to sentence for negligence the illegal handling of a computer virus.

143 Due to its fragmentary character, criminal law is inadequate to maintain the general correctness of information. Only in specific cases, such as for balance sheet items, medical reports or other specific documents, can it guarantee faultless information.

144 For a detailed analyses of the function of "forgery" see *Leng*, Falsity in Forgery, (1989) The Criminal Law Review, pp. 687 et seq.; *Sieber*, Computerkriminalität und Strafrecht, 2nd ed. 1980, pp. 265 et seq.

145 See, e.g., for Austria, Section 223 Penal Code; for Belgium, Section 193 Penal Code; for Germany, Section 267 Penal Code; for France, Section 145 Penal Code; for Italy, Sections 476, 485 Penal Code; for Switzerland, Sections 110, No. 5; 251-7, 317 Penal Code.

146 See for Canada, Section 321 Criminal Code; for Germany, Sections 269, 271, 273, 274, 348 Penal Code, amended in 1986; for Finland, chapter 33 Sections 1-6 of the Penal Code, amended 1990; for France, Article 462-5 and Article 462-6 Penal Code; for Greece, Article 13 C Criminal Code; for

courts in other countries – as in Australia, France, Israel or the Netherlands – came to the same result.[147]

With respect to the correctness and authenticity of information some countries enacted, or are still considering, additional guarantees for new forms of money, especially "plastic money" and prepaid cards (such as telephone cards). These new provisions extend the traditional concepts of counterfeiting money or alteration of securities to new technological developments.

5. Computer Fraud

The preceding paragraphs primarily discussed the questions of whether and in how far the exclusive use, confidentiality, integrity and correctness of information can be a legally protected interest per se. This issue has to be strictly separated from cases where false information is used in order to attack other legally protected interests (such as life or assets).

In most areas of traditional legal interests, the involvement of computer data (e.g., in the case of murder committed by the manipulation of computerised hospital supervision system) does not cause specific legal problems. The respective legal provisions are formulated in terms of results and it is completely irrelevant if this result is achieved with the involvement of a computer or not. However, even in this area computer-specific qualifications are proposed in some countries.[148]

In the field of financial manipulations the situation is different: The statutory definitions of theft, larceny and embezzlement in many legal systems – such as in Germany, Greece, Luxembourg or Japan – require that the offender take an "item of another person's property". The statutory provisions are not applicable if the perpetrator appropriates deposit money; in many countries these traditional provisions also cause difficulties, as far as manipulations of cash dispensers are concerned.[149] The statutory

---

Japan, Articles 7-2, 157, 158, 161-2 Penal Code; for Luxembourg, Articles 509-4 and 509-5 Penal Code; for Norway, Sections 179, 182 Penal Code.

147 See, e.g., for France, Section 150 Penal Code; for Japan, Articles 154-161 Penal Code; for the Netherlands, Section 225 Criminal Code.

148 See, e.g., for the USA, Sections 18.2-152.4 (5) Code of Virginia 1979 making it a crime to use "a computer without authority and with intent to cause physical injury to an individual".

149 See, e.g., for Germany, Sections 242, 246 Penal Code; for Italy, Section 624 Penal Code; for Japan, Articles 235, 252, 253 Penal Code. See for a different result, e.g., in Canada, *R. v. Hardy* (1980), 57 C.C.C. (2d) 73.

provisions of fraud in most legal systems demand a deception of a person. They cannot be used when a computer is "cheated".[150] The statutory definitions of breach of trust or "*abus de confiance*" which exist in several countries – such as in Austria, Belgium, Germany, France, Japan, Luxembourg or Switzerland – only apply to offenders in high positions and not to punchers, operators or programmers; some provisions also have restrictions concerning the protected objects.[151]

Consequently, many Western legal systems looked for solutions *de lege lata* which did avoid stretching the wording of already existing provisions too much.[152] Laws on computer fraud have been enacted in Australia, Austria, Denmark, Germany, Finland, Greece, Luxembourg, Japan, the Netherlands, Norway, Spain, Sweden and the USA.[153] Similar reform proposals are being discussed in the United Kingdom while others are already discussing amending and tightening the existing rules.[154] In addition, the Swedish legislature expanded the provisions on breach of trust to technicians in qualified positions of trust.[155] In general, such legal amendments are necessary since computer-based attacks to traditional legally protected interests should not be privileged.[156]

---

150 See, e.g., for Austria, Section 146 Penal Code; for Denmark, Section 279 Penal Code; for Germany, Section 263 Penal Code; for Italy, Section 640 Penal Code; for Japan, Article 246 Penal Code; for Sweden, chapter 9 Section 1 para. 1 Criminal Code. See for a different result in Belgium, Section 496 Penal Code; in Canada, e.g., Section 380 Criminal Code; in France, Section 405 Penal Code; in the Netherlands, Section 326 Criminal Code.

151 See, e.g., for Austria, Section 153 Penal Code; for Belgium, Section 491 Penal Code; for Germany, Section 266 Penal Code; for France, Article 408 Penal Code; for Japan, Article 247 Penal Code.

152 In most legal systems the principles of legality and of strict interpretation (nullum crimen, nullum poena sine lege; poenalia sunt restringenda) are guaranteed by constitutional provisions. See, e.g., for Germany, Article 103 Basic Law; for the USA, the fifth and fourteenth amendments.

153 See, e.g., for Austria, Section 148a Criminal Code; for Denmark, Section 279a Penal Code, amended in 1985; for Germany, Section 263a Penal Code, amended in 1986; for Finland chapter 36 Section 1 para. 2 of the Penal Code, amended in 1990; for Greece, Article 386 A Criminal Code, amended in 1988; for Luxembourg, Articles 509-2 and 509-3 Penal Code, amended in 1993; for the Netherlands, Article 326c Criminal Code; for Norway, Section 270 (2) Penal Code, amended in 1987; for Japan, Article 246-2 Penal Code; for Spain, Articles 248.2, 239 en fine Criminal Code 1995; for Sweden, chapter 9 Section 1 para. 2 Criminal Code, amended in 1986; for the USA, Section 18 U.S.C. § 1030 (a) (4) (1988) and various state laws.

154 See, e.g., for Germany, the Sixth Bill for the Reform of the Criminal Law of March 1997, Bundestagsdrucksache 13/7164.

155 See for Sweden chapter 10 Section 5 Criminal Code, amended in 1986.

156 For the respective proposals of international organisations see infra chapter IV.

6. Comparative Analysis

Comparing the various legal orders with respect to computer-related economic crime one can state that there exists already a considerable degree of harmonisation. Most countries cover the main forms of computer-related economic crimes (such as computer fraud or sabotage) either by traditional statutes or by new legislation.

However, there are also considerable discrepancies: The most important difference between the various national laws is that some countries – such as Austria, Belgium and Japan[157] – do not have special criminal law provisions against hacking (i.e. the mere penetration into computer systems). Such a criminal offence would be desirable in accordance with existing international recommendations.[158] Considerable differences also exist in the field of trade secret protection. Especially Asian countries still do not pay too much attention to trade secret protection. Even some Western industrialised countries have not yet realised the need to prevent theft of trade secrets and the damage that a lack of protection may cause to the economy. Further differences exist in the field of computer sabotage where most countries have general provisions against (computer) sabotage; however, some countries went further by enacting specific anti-viruses provisions which do not require actual damage or respective intent of the perpetrator.

C. Protection of Intellectual Property

Long before the invention of computers, the doctrine of intellectual property law had discussed the question whether and why specific information should be attributed to its possessor. Theories on the protection of works of authorship go back to the first "privilege of authors" in the 15th century and were especially developed since the end of the 17th century. Today the

157 In Austria, hacking is only punished – according to the respective circumstances – under the aspects of data protection (Section 49 Data Protection Act) and alteration of data (Section 126a Criminal Code), cf. *Schick/Schmölzer*, in: Sieber (ed.), Information Technology Crime, 1994, pp. 26 et seq. In Japan, hacking is, also after the criminal law reform of 1987, only punishable with regard to certain consequences of the offence, e.g., as obstruction of business according to Article 234-2 Penal Code; cf. *Yamaguchi*, in: Sieber (ed.), Information Technology Crime, 1994, pp. 314 et seq.

158 Apart from that, the use of abstract strict-liability offences for the prevention of computer viruses is increasingly being called for; cf., e.g., for Japan *Yamaguchi*, in: Sieber (ed.), Information Technology Crime, 1994, p. 316.

concept of "intellectual property law" is based both on the recognition of "natural rights" in intellectual property and on the pragmatic reason of stipulating the creation of works of authorship by granting a certain premium to its creator.

In the field of information technology this concept is especially important for the protection of computer programs, semiconductor topographies and databases: After computer programs had been excluded from patent protection throughout the world in the 1970s, various countries at first passed new laws which assured a civil law copyright protection for these programs (infra 1). Since 1984 additional laws for the protection of topographies of semiconductor chips were adopted (infra 2). Special legal protection on databases was first enacted in 1997 (infra 3). More severe provisions of criminal copyright law entered into force in numerous legal systems since the mid 1980s (infra 4).

1. Computer Programs

With respect to computer programs, trade secret protection – as well as contract protection – not only applies to all computer-stored data, but is also an important means for protection. However, since these legal devices are restricted to secret programs, special relationships and/or specific acts of accessing information, they are not sufficient in guaranteeing untroubled trade with computer programs. The discrepancy between the costs of computer programs and those of reproducing them is so vast that there was a strong demand in all countries for a further-reaching protective system which includes non-secret programs and applies to third parties.[159] As patent law can only protect a small number of programs which include a technical invention,[160] the discussion has focused in all countries on the applicability of copyright law.[161]

159 See *Sieber*, Copyright Protection of Computer Programs in Germany, (1984) European Intellectual Property Review, p. 214 at 253.

160 See the references supra chapter I, fn. 22 and the comparative overview of *Hannemann*, The Patentability of Computer Software – An international guide to the protection of computer-related inventions, 1985.

161 In addition to existing provisions, special protective structures for computer programs have been discussed mainly by the governments of Japan and of France, but have been abandoned in favour of the copyright option mentioned above. See *Sieber*, The International Handbook on Computer Crime, 1986, pp. 72 et seq. A sui generis provision only on the criminal protection of computer programs (not depending on its copyrightability) was enacted by the Greek legislature in 1988. See for *Greece*, Article 370 C (1) Criminal Code, as amended by Law 1805/88.

With the aim of avoiding legal uncertainty, most countries have explicitly provided copyright protection for computer programs by legislative amendments since the 1980s. This has been the case e.g. in Australia, Austria, Brazil, Canada, Denmark, Germany, Finland, France, Hungary, Israel, Japan, Luxembourg, Malaysia, Mexico, the Philippines, the Republic of China, Singapore, Spain, Sweden, the United Kingdom and the USA.[162] As a consequence, in all countries, the courts recognise copyright protection of computer programs today. This fundamental recognition of the inclusion of computer programs in copyright protection was strongly promoted by the EC Directive on the protection of computer programs and by other international proposals in this field.[163]

The work of international and supranational organisations has also led to a considerable degree of harmonisation with respect to the scope of copyright protection. This concerns e.g. the acts covered by copyright law, the distinction between inadmissible adaptation and permissible fair use, the admissibility of back-up copies and private copying, the duration of protection, and the authorship as well as the applicability of moral rights. This report will not go into the details of these questions since they primarily belong to the domain of civil law. However, since most penal provisions on copyright offences refer to the respective civil provisions, these civil law problems also determine the range of the respective criminal offences.

2. Semiconductor Products

Computer programs are not the only new economic values created by modern computer technology. With regard to the miniaturisation of computers and the development of "fifth generation" computers, the technique of integrated circuits has become more and more sophisticated. Due to the possibilities of copying the topography of semiconductor products, there is a demand for an effective protection of such products in order to stop unauthorised reproduction.

In most countries, it remained unclear as to what extent the topography of semiconductor products was protected against reproductions by patent law, copyright law, registered designs, trade secret law and competition law. In the United States a special protection for computer chips was provided by the Semiconductor Chip Protection Act of 1984. In Japan, a similar law was

162 For the respective countries and for references see supra chapter I, fn. 23.

163 Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs, OJ L 122/42 of 17.05.1991. For details see infra chapter IV.C.1.

passed in 1985. As a result of a respective 1986 EC Directive,[164] special laws protecting the topographies of semiconductor products were also enacted in various countries of Europe, e.g., in Austria, Denmark, Germany, France, Italy, the Netherlands, Spain, Sweden and the United Kingdom.[165] The passing of semiconductor chip laws in the Member States of the European Union after 1986 shows that the possibility of the European Community to pass binding directives leads to a new age of legal harmonisation and a *ius commune* in Europe.[166]

Contrary to the law of the United States and to the Italian law, the Austrian, Dutch, Finnish, German, Japanese and Swedish laws include criminal sanctions which, among other things, punish the infringement of a circuit layout right.[167] Such penal sanctions for clear cases of infringements of circuit layout rights seem to be appropriate.

3. Databases

A new field for copyright as well as sui generis protection has become the legal protection of databases. In Europe a 1996 Directive on the legal protection of databases[168] will lead to a parallel legal development in all Member States. E.g., Germany enacted its amendments to the Copyright Act in 1997 providing for a new comprehensive *sui generis* protection of databases.[169]

4. Criminal Law

Apart from the criminal law problems originating from the sphere of civil law, the role of penal protection of intellectual property was evaluated

164 Council Directive 87/54/EEC of 16 December 1986 on the legal protection of topographies of semiconductor products, OJ L 24/36 of 27.01.1987; cf. infra chapter IV.C.2.

165 See supra chapter I, fn. 25.

166 Cf. *Coing*, Europäisierung der Rechtswissenschaft, (1990) Neue Juristische Wochenschrift, p. 937.

167 See, e.g., for Germany, Section 10 of the Act on the Protection of Topographies of Micro-electronic Semiconductor Products of 22 October 1987 (Bundesgesetzblatt I, p. 2294, as amended 1990); for Finland, Section 35 of the Act on the Protection of Semiconductor Topographies No. 32/1991 of 11 January 1991 and chapter 40 Section 2 of the Penal Code (as amended in 1995); for the Netherlands, Article 24 of the Act of 28 October 1987 on the Protection of Original Topographies of Semiconductor Products.

168 Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, OJ L 77/20 of 27.03.1996.

169 See, for Germany, Article 6 of the Information and Communication Services Act 1996.

differently in various countries for many years. While the copyright law in common law systems did not or only rarely resort to penal sanctions, civil law systems generally punished infringements of copyright by lenient criminal sanctions. The increase in music, video and program piracy in recent years has removed most of these differences since many countries are now creating effective criminal deterrents. Although some of the new laws are still confined to phonographic products, most of them are of a general nature.

An international tightening of criminal copyright law can be observed in a number of countries since 1981. Reforms to mention are in particular those in Italy of 1981, in United Kingdom of 1982, in Sweden and in the USA of 1982, in Finland of 1984, in Denmark and France of 1985, in Canada of 1987, in the United Kingdom of 1988 and in Hungary of 1992.

This tightening of criminal law was not so much based on the activities of international organisations, but on the new need for protection in the information society, which brought about – against the background of a changed *Zeitgeist* – an improved protection of intellectual property by criminal law. These changes and efforts towards a more effective penal copyright protection are justified, since attacks against intellectual property deserve the same attention of penal law as the more conventional attacks on corporeal property. The reluctance to criminalise copyright infringements which still prevails in some common law countries should be counteracted by adequate civil law provisions. These provisions should limit criminalisation only to severe cases that either cause economic damage or are regularly committed for gain.[170]

5. Comparative Analysis

The protection of intellectual property both by civil law and by criminal law was extended considerably in the whole world during the last decade. In this field, the law has reacted to the shift from the industrial to the information society in a remarkable manner. This has been the case especially with respect to computer programs and semiconductor products and is presently happening in the field of databases. But while civil remedies against violations of intellectual property rights have already received a considerable amount of comparable treatment in the countries surveyed, criminal copyright law and criminal protection of *sui generis* legislation still show

170 For the proposals of international organisations in the field of penal copyright protection see infra chapter IV.C.

considerable differences and its general necessity is not commonly accepted in all countries.

D. Illegal and Harmful Contents

In the 1990s, a new complex of issues raised considerable importance in the field of substantive law. The dissemination of pornography, racist statements, as well as information glorifying violence, in particular via the Internet, put the question as to what extent these offences could be confronted with the help of criminal law. With respect to this question, two legal issues have to be distinguished: The first one concerns the criminal liability of the author or the content provider of the respective statement (infra 1). The second one is about the additional liability of the service provider whose networks and/or servers are abused by third parties (infra 2).

1. Criminal Liability of the Content Provider (Using the Example of Child Pornography)

Illegal contents in international computer networks can be subject to a number of statutory provisions. The majority of illegal contents on the Internet concerns pornography; however, there are also cases of hate speech, glorifying of violence, racist statements or libel. The various national legal systems treat these offences quite differently. Since it is not possible to compare all of these (generally non-computer-specific) offences, the following chapter will discuss the relevant problems using the example of pornography especially in the field of child pornography. This example illustrates the variety of legal statutes in the area of illegal contents as well as the need to extend the scope of the respective statutes on illegal and harmful contents not only to traditional writings but also to computer devices.

a. Differing Concepts against Pornography

In most countries (especially in continental Europe) the basic penal provisions against child pornography are regulated in the national penal codes.[171] However, in some countries there are also special laws on

171 See, e.g., for Germany, Section 184 Criminal Code; for Spain, Article 186 Criminal Code; for Italy, Sections 528, 529, 725, 726 Criminal Code; for Belgium, Articles 383, 384, 383 bis Criminal Code.

pornography.[172] In other countries, laws for the protection of minors[173] or laws on telecommunication[174] are also applicable. Moreover, media laws (e.g. press laws) possibly apply and have to be taken into consideration.[175]

A comparative analysis of these laws has to start with an analysis of the basic concepts of these provisions, since the most important differences among the penal regulations against pornography are not based on different legal techniques, but on different legal interests and different goals of the national conceptions against pornography. An analysis of these basic concepts shows that the national legal systems protect mainly four different legal interests:

- The narrowest concept of protection aims exclusively at the protection of children and other persons requiring similar protection against exploitation as actors in pornographic scenes.[176] In several legal systems this so-called "actors' protection" is extended victims of violence and to animals.[177] However, sometimes it remains unclear whether the penal provision only protects the actor who is directly victimised or whether its goal is also to prevent imitation of such conduct.
- A second concept of protection is also directed at the protection of minors but focuses on the protection of the mental and moral development of

172 See, e.g., for Austria, Federal Act of 31 March 1950 against Obscene Publications and for the Protection of the Young People; for the UK, Obscene Publications Act 1959; for Finland, Prevention of Dissemination of Indecent Publications Act 1927.

173 See, e.g., for Germany, Law on the Dissemination of Publications and Other Media Morally Harmful to Youth; for the UK, Protection of Children Act 1978; for the Republic of Ireland, Child Pornography Act 1996.

174 See, e.g., for the USA, the Communications Decency Act 1996.

175 The following description mainly considers the basic penal laws as well as laws specifically fighting pornography and provisions in telecommunication statutes with respect to their applicability in the fight against child pornography.

176 See, e.g., for Austria, Section 207a Criminal Code; for Belgium, Article 383 Penal Code; for Canada, Section 163.1 Criminal Code; for Denmark, Section 235 Criminal Code; for France, Article 227-23 New Penal Code; for Germany, Section 184 (3) Criminal Code, for Ireland, Section 2 Child Pornography Act 1996; for the Netherlands, Section 240b Criminal Code, for Norway, Section 211 Criminal Code; for Spain, Article 189 1 Criminal Code; for Sweden, chapter 16 Section 10a Criminal Code; for the UK, Section 1 of the Protection of Children Code 1978 as amended by the Criminal Justice and Public Order Act 1994; for the USA, 18 U.S.C. § 2252.

177 See, e.g., for Denmark, Section 235 Criminal Code; for Germany, Section 184 (3) Criminal Code; for Norway, Section 211 (6) Criminal Code; for Sweden chapter 16 Section 10b (2) Criminal Code.

young people. This concept aims e.g. to protect minors against being handed over, or getting access to, pornographic publications.[178]

- Another concept of protection which also extends to adults wishes to enforce fundamental principles of human dignity by protecting the unsuspecting general public from incidentally being confronted with pornography.[179]
- In an even broader concept, numerous countries try to maintain certain public moral standards.[180] Sometimes this concept of protection is specified to protect the general morals of the society.

These four general directions and concepts of anti-pornography laws in the different legal systems are combined with each others in various ways:

- In several countries (e.g. Belgium, Finland) only the protection of minors by one or both of the above mentioned first two concepts of protection is acknowledged as a legal interest.[181]
- Other legal systems add the protection of adults against undesired confrontation with pornography as an additional legal interest.[182] Doing this, the combination of the various legal interests is realised by different legislative techniques. In contrast to the complicated and intricate legal situation in Germany, the Criminal Code of the Netherlands differentiates according to a clear protection conception: Every one of the concepts of

178 See, e.g., for Denmark, Section 234 Criminal Code; for Germany, Section 184 (1) Criminal Code, Sections 1, 21 of the Law on the Dissemination of Publications and Other Media Morally Harmful to Youth; for Greece, Article 30 of the Law 5060/1931 related to the Punishment of Immodest Behaviour; for Spain Article 186 Criminal Code; for Sweden, chapter 16 Section 12 Criminal Code; for Switzerland, Article 197 Criminal Code.

179 See, e.g., for Canada, Section 163 Criminal Code; for Denmark Sections 232, 233, 234 Criminal Code; for Finland, chapter 20 Section 9 Penal Code, Section 1 para. 1 of the Prevention of Dissemination of Indecent Publications Act 1927; for France, Articles 227-24, 227-28, R 624-2 New Penal Code; for Greece Articles 29 (1), 30 of the Law 5060/1931 related to the Punishment of Immodest Behaviour; for Germany, Section 184 (1) Criminal Code, Section 1 and 21 of the Law on the Dissemination of Publications and Other Media Morally Harmful to Youth; for Ireland, Section 2 (1) (b) of the Child Pornography Act 1996; for Japan, Article 175 Penal Code; for Norway, Sections 376, 377 Criminal Code; for Sweden, chapter 16 Section 10b and Section 12 Criminal Code; for the UK, Section 1 (1) of the Protection of Children Act as amended by the Criminal Justice and Public Order Act 1994.

180 See, e.g., for Denmark Section 232 Criminal Code; for France, Article R 624-2 New Penal Code; for Greece, Article 29 (1) of the Law relating to the Punishment of Immodest Behaviour; for the Netherlands, Section 240 Criminal Code; for Norway Sections 376, 377 Criminal Code. In Italy even the Constitution (Article 21 Section 6) calls for the protection of public morality.

181 See for Belgium, Article 384 Penal Code.

182 E.g. Canada, Denmark, Finland, France, Germany, Ireland, Norway.

protection is addressed in a separate statutory provision. The advantage of this is that each provision can be applied with special regard to the respective protected legal interest.[183]

– The provisions of countries that also cover the protection of moral standards usually do not only include these legal interests but reach far beyond these interests.[184] In legal systems where such wide concepts of protection are applied, it is often argued that such penal provisions lack the necessary clarity and preciseness. However, such general concepts of protection are retreating in continental Europe.

It is clear that these different national concepts against pornography lead to considerable differences in the respective legal provisions. However, even in countries with similar concepts and traditions the criminal provisions vary considerably. This can be exemplified for the field of child pornography in the following.

b. Provisions on Child Pornography

The dissemination of publications containing child pornography is punishable under all of the above mentioned concepts and in all examined legal systems. Especially the last few years have produced a trend towards extending the penal protection against child pornography by special provisions. As a consequence in most countries nowadays exist special penal provisions against child pornography.[185] Only in a few countries, the dissemination of child pornography is still covered by general provisions against pornography.[186]

The age of the children protected by the provisions against child pornography differs considerably. E.g., when it comes to protecting minors from being exploited as actors, the age limit is 14 years in Austria and

183 In the Criminal Code of the Netherlands, Section 240 protects against undesired confrontation with sexual publications, Section 240a protects against mental misdevelopment of youngsters and Section 240b protects youngsters against performing in pornographic photos, pictures and films.

184 See, e.g., Greece, Norway, USA.

185 See, e.g., for Austria, Section 207a Criminal Code; for Belgium, Article 383 Penal Code; for Canada, Section 163.1 Criminal Code; for Denmark, Section 235 Criminal Code; for France Article 227-23 New Penal Code; for Germany, Section 184 (3) Criminal Code, for Ireland, Section 2 Child Pornography Act 1996; for the Netherlands, Section 240b Criminal Code, for Norway, Section 211 Criminal Code; for Sweden, chapter 16 Section 10a Criminal Code; for the UK, Section 1 of the Protection of Children Code 1978 as amended by the Criminal Justice and Public Order Act 1994.

186 E.g., in Finland, Italy, or Luxembourg. In Italy and Finland, special provisions against child pornography are being discussed at the moment.

Germany, 15 years in France and Poland, 16 years in Belgium, Switzerland, the Netherlands, Norway and the United Kingdom and 18 years in Canada, Sweden, and the US.[187] Sometimes other persons requiring protection similar to the one given to minors are also included. In many countries the liability for "hard-core" pornography is not limited to child pornography, but also covers pornography combined with excessive use of violence,[188] sodomy,[189] negrophilia or sexual presentations involving human secretions. Sometimes depictions not portraying an actual case of sexual child abuse (e.g. simulated computers animation, so-called "morphing") are also penalised.[190]

Some legal systems merely cover visual depictions of pornography. Other legal systems include sound recordings as well. In several legal systems it has been discussed to what extent depictions on computer networks may be treated the same as depictions on paper. Some countries have amended their respective laws to include pornographic material on computer storage devices.[191] Therefore, most countries currently penalise storing pornographic material in computer systems on discs and tapes.[192] Thus, there is consensus that depictions which are illegal on paper should also be illegal if stored and used on computers. But it is not yet possible to comment how far the penal provisions can be extended to cover mere depictions on computer screens as well as video sequences.

The punishable acts of child pornography include the dissemination, the providing with and the publishing of child pornography. Moreover, in recent years there is a trend to extend the penal provisions also to the possession of child pornography.[193] At the moment, some countries are discussing draft

187 See for Austria Section 74 Criminal Code; see for Belgium, Article 383 bis Penal Code; see for Canada, Section 163.1 (1) (a) (ii) Criminal Code; see for France, Article 227-23 New Penal Code; see for Germany, Section 176 Criminal Code; see for the Netherlands, Section 240b Criminal Code; see for Norway, Section 211 (1) (d) Criminal Code; see for the USA, 47 U.S.C. § 223 (a).

188 See, e.g., for Canada, Section 163 (8) Criminal Code; for Norway, Section 211 (2).

189 See, e.g., for Denmark, Section 235 (2) Criminal Code; for Norway, Section 211 (2).

190 See, e.g., for Austria, Section 207a Criminal Code; for Canada, Section 163.1 Criminal Code and (since 1997) for Germany, Section 184 (4) Criminal Code.

191 See, e.g., Ireland, Section 1 of the Child Pornography Act 1996; for Germany, Section 11 (3) Criminal Code, for the UK, Section 7 (4) of the Protection of Children Act 1978 as amended by the Criminal Justice and Public Order Act 1994.

192 See, e.g., for Austria, Section 207a (3) Criminal Code; for Belgium Article 383 Penal Code; for Denmark, Section 235 (2) Criminal Code; for Germany, Section 184 (1) Criminal Code; for Norway, Section 211 (1) (d).

193 See, e.g., for Austria, Section 207a (3) Criminal Code; for Belgium, Article 383 bis Penal Code; for Germany, Section 184 (5) Criminal Code. In the USA, 18 U.S.C. § 2252 (a) (4) punishes possession only if at least three publications with child pornographic content are possessed.

bills incorporating the possession of child pornography in new penal provisions. Thus, the number of countries without any provisions against the possession of child pornography is decreasing. If the difficulties in prosecuting the authors of illegal contents in international computer networks continue, the trend to extend criminal liability to the "consumers" of child pornography may become even stronger.

c. General Provisions against Pornography

The general penal provisions against the dissemination of other forms of pornography (especially against providing such material to minors and adults) differ even more than the provisions against child pornography. Differences exist even between neighbouring countries where a certain common understanding of cultural and moral values and ideas might be expected: For example in Norway, there are considerably more restrictive rules on pornography than in Sweden. This resulted in Norway prohibiting cable TV broadcasts of Swedish movies.

All legal systems face the problem that the exact scope of the concepts of "pornography", "obscenity" or "indecency" is almost impossible to determine. Therefore, future scientific comparison of the corresponding penal provisions will also have to include an analysis of the relevant national case law.

d. Other Communication Offences

A great diversity and variety of provisions can be found when examining provisions on incitement to violence,[194] hatred[195] or racism.[196] These statutory provisions protect additional legal interests such as human dignity and public peace besides also providing protection to minors. Summing up one can say that the scope of illegal and harmful contents shows considerable discrepancies in the various national laws.

194 See, e.g., for Canada, Section 318 Criminal Code; for Germany, Section 111 Criminal Code; for Switzerland, Article 135 Criminal Code.

195 See, e.g., for Canada, Section 319 Criminal Code; for Ireland, Section 2 of the Prohibition of Incitement of Hatred Act 1989; for Spain, Article 510 Criminal Code.

196 See, e.g., for Spain, Article 607.2 Criminal Code; for Portugal, Articles 239, 240 Criminal Code; for Sweden, chapter 16 Section 8 Criminal Code; for Switzerland Article 261 bis Criminal Code; for the UK, Section 19 Public Order Act 1986.

2. Responsibility of Access and Service Providers

The criminal liability of the author of statements containing illegal contents as described above must be distinguished from the issue of an additional co-liability of service and access providers for the statements disseminated via their computer systems and data networks. It is no surprise that in most countries, this issue of co-liability of service and access providers is being discussed controversially and legal analysis is still at a very early stage.

After a first phase of discussion in which the issue was dealt with in a general and often controversial way,[197] a number of countries have engaged in or are starting to engage in a more detailed and differentiating analysis of the issue. However, up to now only a few countries (USA, Germany, Sweden) have adopted or proposed new legislation along these lines.[198] Other countries (e.g. the Netherlands and the Nordic countries) try to apply existing rules of criminal law and other relevant laws (such as telecommunication laws) to the issues raised by the new technological phenomenon of Internet access and service providers.[199] Especially since 1997, the new laws as well as court decisions and the academic discussion are characterised by a differentiation taking up the various functions performed by Internet service providers, access providers and online services (such as the responsibility for proprietary contents, for storing third–party content, and for merely providing access functions or network services to third parties).[200] The main differentiating line is drawn between

197 See, e.g., for Germany, the analysis of *Sieber*, Strafrechtliche Verantwortlichkeit für den Datenverkehr in internationalen Computernetzen, (1996) Juristenzeitung, pp. 429 et seq., 494 et seq.; *Bleisteiner*, How Germany is Dealing with Free Speech over the Internet, (Volume XIII, No. 7, November 1996) Computer Law Strategist, pp. 5 et seq.; for the USA, Denning/Lin (eds.), Rights and Responsibilities of Participants in Networked Cummunities, 1994, especially pp. 55 et seq; *Perritt*, Law and the Information Highway, 1996, pp. 161 et seq.; Smedinghoff (ed.), Online Law, 1996, pp. 301 et seq. Also comparative study by *Middleton*, Liability of Service Providers for Defamation in Cyberspace, (1997) European Business Law Review, pp. 108 et seq.; *Bortloff*, Neue Urteile in Europa betreffend die Frage der Verantwortlichkeit von Online-Diensten, (1997) Zeitschrift für Urheber- und Medienrecht, pp. 167 et seq.

198 See, for Germany, Section 5 Teleservices Act and Section 5 State Treaty of the German Länder on Media Services and *Sieber*, Kontrollmöglichkeiten zur Verhinderung rechtswidriger Inhalte in Computernetzen, (1997) Computer und Recht, pp. 581 et seq., 653 et seq.; for the USA, 47 U.S.C. § 223, 47 U.S.C. § 230. Sweden has proposed an Electronic Mediation Services Act in 1996.

199 See, e.g., for Austria, Section 43 Telecommunications Act; for the Netherlands, Articles 53, 54, 418, 419 Criminal Code. See also the study of the *OECD, DSTI/ICCP(97)14*, Approaches to Content on the Internet, pp. 21 et seq. (hectography only).

200 Accordingly the legal evaluation has resulted in a multi-layered set of rules on the responsibility for illegal online content: In all countries it is clear that it is the author or content provider who is the primary target of rules on the responsibility for illegal content. Secondly a provider may be

service providers storing third party content on their own servers on the one hand, and mere access and network providers which only transport third party content and provide users with the possibility and the technical capabilities to use an international data network on the other hand.

- With respect to the responsibility of service providers, a tendency seems to emerge that favours a liability limited to instances where the service provider has actual knowledge about a specific illegal content on his server and where it is technically feasible and can reasonably be expected from the provider to erase such content. This approach is e.g. reflected in Section 5 (2) of the German Teleservices Act. It states that "providers shall not be responsible for any third-party content which they make available for use unless they have knowledge of such content and are technically able and can reasonably be expected to block the use of such content."[201] However, this approach is not uncontested: In some countries courts have taken an even more restrictive view and have held that a service provider may only be liable under even more limited circumstances. Other countries show a tendency for a more severe regime of liability.[202]
- With respect to mere access and network providers, it is mostly agreed upon that they should not be held liable for the content they provide access to and transport via their computer systems.[203] Due to the special technical and legal circumstances that do not allow them to perform the necessary actions of supervision and control over such content, it is not considered appropriate to even allocate a basic responsibility to these providers. Consequently Section 5 (3) of the German Teleservices Act states that "providers shall not be responsible for any third-party content to which they only provide access."[204] Some countries (e.g. Austria,

---

held liable who's servers are used to store and keep available the incriminated content. A possible liability of access or even network providers would have to be considered as a last option to allocate criminal liability.

201 For details see *Sieber*, Kontrollmöglichkeiten zur Verhinderung rechtswidriger Inhalte in Computernetzen, (1997) Computer und Recht, pp. 581 et seq., 653 et seq. A similar provision can be found in Section 5 (2) State Treaty of the German Länder on Media Services. See also for the USA, 47 U.S.C. § 223 (e) (3).

202 See *Bortloff*, Die Verantwortlichkeit von Online-Diensten, (1997) Gewerblicher Rechtsschutz und Urheberrecht Int., pp. 387 et seq.

203 See, e.g., for the USA, 47 U.S.C. § 223 (e) (1), 47 U.S.C. § 230 (c) (1). See also *Kaspersen*, Liability of Providers of the Electronic Highway, in: European Commission, Legal Advisory Board (ed.), Convergence between telecommunications and audiovisual: consequences for the rules governing the information market, 30 April 1996, pp. 39 et seq. (hectography).

204 Section 5 (3) also states that "the automatic and temporary storage of third-party content due to user request shall be considered as providing access." A similar provision can be found in Section 5 (3) State Treaty of the German Länder on Media Services. See *Sieber*,

Greece) have arrived at the same conclusion using and applying traditional legal concepts. Some legal systems, however, extend or discuss extending liability also to access providers especially with respect to specific narrow exemptions.[205] In Germany Section 5 (4) of the Teleservices Act allows an injured party to bring claims against an access provider if the remedy sought is a cease and desist order.[206]

Taking into account the legal development in some Asian countries such as Vietnam, the Republic of China and Singapore as well, it becomes clear that the various national laws do not only show a different understanding of the technical issues involved, but also are based on substantially different concepts and positions with respect to the value of (transborder) freedom of information.[207] Where this basic civil right is considered to be of less importance or is even considered being dangerous to the safety and integrity of a country's attempts to invoke censorship, an extension of criminal liability beyond technically sound limits is being discussed and implemented. This view stands in sharp contrast to the appreciation of the freedom of information that prevails in Western democracies.[208]

Kontrollmöglichkeiten zur Verhinderung rechtswidriger Inhalte in Computernetzen, (1997) Computer und Recht, pp. 581 et seq., 653 et seq.

205 See, e.g., Sections 1, 5, 6 of the Swedish Electronic Mediation Services Bill of 1996; for Switzerland, Entscheidungssammlung des Schweizerischen Bundesgerichts, Volume 121, 1995, IV, p. 109; *Sieber*, Strafrechtliche Verantwortlichkeit für den Datenverkehr in internationalen Computernetzen, (1996) Juristenzeitung, pp. 429 et seq., 494 et seq. (at 499).

206 Section 5 (4) Teleservices Act states: "The obligations in accordance with general laws to block the use of illegal content shall remain unaffected if the provider obtains knowledge of such content while complying with telecommunications secrecy under Section 85 of the Telecommunications Act and if blocking is technically feasible and can reasonably be expected."

207 See, e.g., for Singapore, *Chandram*, Internet Regulation in Singapore, (1996) CLSR, p. 410.

208 This later approach was highlighted by the consenting opinion of Justice *Dalzell* in the above mentioned CDA decision in the US. See ACLU vs. *Reno*, 929 F. Supp. 824, 883 (E.D.Pa. 1996):

"Cutting through the acronyms and argot that littered the hearing testimony, the Internet may fairly be regarded as a never-ending world-wide conversation. The Government may not, through the CDA, interrupt that conversation. As the most participatory form of mass speech yet developed, the Internet deserves the highest protection from governmental intrusion. True it is that many find some of the speech on the Internet to be offensive, and amid the din of cyberspace many hear discordant voices that they regard as indecent. The absence of governmental regulation of Internet content has unquestionably produced a kind of chaos, but as one of plaintiffs' experts put it with such resonance at the hearing: What achieved success was the very chaos that the Internet is. The strength of the Internet is that chaos. Just as the strength of the Internet is chaos, so the strength of our liberty depends upon the chaos and cacophony of the unfettered speech the First Amendment protects. For these reasons, I without hesitation hold that the CDA is unconstitutional on its face."

Some countries such as Australia, Belgium, Germany, the Netherlands and the United Kingdom have tried to solve this potential conflict of freedom of speech and the protection of vital public interests by encouraging or mandating industry codes of conduct or other forms of industry self-regulation mechanisms. Some of these models are based on private initiatives and provide some sort of hotline service to users wishing to report illegal activity on the Internet.[209] Often these groups and organisations receive some degree of governmental backing and support. Others have been mandated by law. In Germany, e.g., Section 7a of the Law on the Dissemination of Publications Morally Harmful to Minors has been created requiring anyone who "makes available, on a commercial basis, electronic information and communication services which are based on transmission by means of telecommunication" to either appoint a commissioner responsible for the protection of minors if such services are generally available and might include content morally harmful to minors, or to meet this obligation by joining a self-regulation organisation to take over these duties.[210] In the United States the implementation of "good Samaritan" blocking and screening is encouraged by excluding liability with respect to such measures.[211]

3. Comparative Analysis

A comparative analysis with respect to illegal contents has to differentiate between provisions belonging to the special part of criminal law regulating specific crimes (such as the provisions on pornography or hate speech) and the ones addressing the issue of co-liability of access and service providers:

– As far as special criminal provisions are concerned, the national laws examined for this report in the field of pornography show huge differences with respect to the protected legal interests and the scope of these statutes. They vary, e.g., when one analyses specific statutory requirements such as the age of protected children with respect to child pornography or the exact definition of the term pornography and its

209 See, e.g., in the Netherlands the "Meldepunt Kinderpornografie" at <http://www.meldpunt.org> (accessed on 21 January 1998) in the UK the activities of the Internet Service Providers Association (ISPA-UK) at <http://www.ispa.org.uk> (accessed on 21 January 1998) and of the Internet Watch Foundation at <http://www.internetwatch.org.uk> (accessed on 21 January 1998); in the USA the "Cyberangels" at <http://www.cyberangels.org> (accessed on 21 January 1998). See also the comparative Analysis of Hydra Associates, The Protection of Minors and Human Dignity in the Information Society, 1996, Volume 2 (Hectography); European Comission, DG XIII, Interion Report on Initiatives in EU Member States with respect to Combating Illegal and Harmful Contents on the Internet, 4 June 1997, WPIC 16/97 (revised 2), pp. 6 et seq. (hectography).

210 A similar provision can be found in Section 8 (4) State Treaty of the German Länder on Media Services. Such a body, the "Freiwillige Selbstkontrolle Multimedia Diensteanbieter e.V. (FSM)", was established in the summer of 1997, see at <http://www.fsm.de> (accessed on 21 January 1998).

211 See, 47 U.S.C. §§ 223 (e) (5), 230 (c) (2).

various derivatives.[212] However, despite these huge differences in existing laws, there are some common tendencies in many countries. These are in particular directed towards extending or clarifying the applicability of penal statutory provisions with respect to activities within computer networks,[213] increasing the criminalisation of child pornography, criminalising possession of child pornography and creating a clearer system of protected legal interests in criminal provisions covering pornography (in part giving up overly broad concepts of protecting public morals).

– With respect to the co-liability of service, access and network providers, one can state that considerable uncertainties and differences in the allocation of liability for these persons exist. Only a few countries have started to specifically address the issue and consider its specific technical and functional aspects with respect to international data networks. In many jurisdictions, it is still a rather open question as to which facts should be taken into account and what balance should be found when considering conflicting interests. Among the factors that are considered are whether providers act as a mere conduit or whether they are involved in supplying content, their degree of knowledge of illegal contents, their actual abilities to exercise control, as well as the longevity of the incriminated information. For that reason, it is only possible to analyse a certain tendency in the development of the respective national laws: Service providers are mostly held responsible for a specific illegal content on their servers in cases of knowledge, and access providers are generally not held liable for third party content to which they only provide access.

Given the international and world-wide scale of modern computer networks such as the Internet, this leads to a substantial amount of uncertainty as to

212 For the constitutional implications of, e.g., outlawing "indecency" see for the USA, the provisions of the Communications Decency Act of 1996 and the respective court decisions (e.g. ACLU vs. *Reno*, 929 F. Supp. 824 (E.D.Pa. 1996), aff'd. 117 S. Ct. 2329 (1997); *Shea* vs. *Reno*, 930 F. Supp. 916 (S.D.N.Y. 1996)) striking down these provisions as unconstitutional.

213 The author, content provider or producer of illegal contents is generally speaking fully liable for such content. The dissemination of such content on computer networks should not be privileged compared to the dissemination of such content in traditional media such as books, CDs or videos. Often this finding is referred to as: "What is illegal off-line has to be illegal online as well." On the other hand it is often pointed out that the liability standards on new electronic media are not to be drawn wider than in traditional media either. These rules apply of course also to service and access providers who produce content of their own. In Germany Section 5 (1) of the Teleservices Act reflects these findings by clarifying that "providers shall be responsible in accordance with general laws for their own content, which they make available for use". A similar provision can be found in Section 5 (1) State Treaty on the German Länder on Media Services.

the most basic legal requirements for operating an online service or other functions within international computer networks. These impediments to the development of a viable online-industry will have to be addressed on an international level in order to achieve at least a minimum of standards accepted in all countries participating in such computer networks. Such international co-ordination could avoid a "race to the bottom" where the countries with the lowest standards would become the ideal host-countries for storing and making available of contents that are illegal elsewhere.

E. Criminal Procedural Law[214]

1. Relevance and Historical Development

Computer-specific procedural law problems are not only important for the prosecution of computer crime cases, but in many other fields of criminal investigation. This is especially illustrated by the prosecution of economic crimes mainly in the banking area, where most of the relevant evidence is stored in automated data-processing systems. Similarly, perpetrators in the field of organised crime increasingly make use of computer systems and transfer data to computers abroad via telecommunication networks in order to render access more difficult for the prosecution authorities. Also in the field of "traditional" crime, computer-stored evidence is already relevant, as is illustrated by cases of drug traffickers conducting their business by using personal computers and international telecommunication systems.[215] New optical storage devices based on compact disc technology encourage even more that "originals", if they still exist at all, be recorded in automated data processing systems and then be destroyed.

214 The following chapter is based on a report originally prepared for the Council of Europe's Select Committee of Experts on Computer-Related Crime (see *Sieber*, Procedural Law Problems with Regard to the Use of Computerized Data in Criminal Investigations, Council of Europe, Report No. PC-R-CC-89-3 of 23 February 1989); a slightly modified version of this report is incorporated as chapter III in the Council of Europe's final activity report on "Computer-Related Crime" of 1990; an updated version was published in *Sieber*, The International Emergence of Criminal Information Law, 1992, pp. 41 et seq.

215 On the contrary, the frontiers of computer-related criminal procedural law are passed, where only electronic measures without connection to data or information are concerned, so in the utilisation of hidden microphones; cf. for example in Germany Article 100c Criminal Procedural Code (see for this provision also Bundesverfassungsgericht, (1997) Neue Juristische Wochenschrift, p. 1018).

Due to these new technical developments and to the growing use of computers in all areas of economic and social life, courts and prosecution authorities depend to an increasing extent on evidence stored or processed by modern information technology. The replacement of visible and corporeal objects of proof by invisible and intangible evidence in the field of information technology does not only create practical problems but also opens up new legal issues. Especially since the beginning of the 1990s the world of IT has become even more complicated by the liberalisation of the telecommunication markets and the wide expansion of the Internet. In the field of coercive powers one has to consider e.g. that in new media and modern forms of communication the distinguishing between the classical categories of individual communication, mass communication and even mass media (which is of great importance for the relevant personal rights and coercive powers) has become difficult.[216]

The following chapter will discuss the main computer-specific questions associated with collecting and using evidence in the field of information technology: the coercive powers of prosecuting authorities to gather evidence in the field of information technology (infra 2), the specific problems of gathering, storing, and linking personal data in criminal proceedings (infra 3), the admissibility of evidence originating from computer records in criminal court proceedings (infra 4), as well as the "extraterritorial" application of national computer-crime statutes (infra 5). These topics raise new computer specific problems in all legal systems which, in addition, are also relevant to the functioning of international mutual assistance[217] and co-operation (infra 6).

---

216 For a long time these legal issues have not been dealt with in detail. In all countries, the discussion of the legal consequences of computers for criminal law focused on substantive law and neglected procedural law aspects. This is documented by the fact that during the last three decades, a great number of countries created special data protection laws and new acts fighting computer crime with substantive criminal law, but only a few countries developed new legal provisions concerning investigations in computerised environments. Similarly, in most legal systems there are many court decisions, books, and articles on data protection law and the substantive law aspects of computer crime, but few decisions and articles deal with the relevant procedural issues. For the first comparative analysis of these procedural law questions see *Sieber*, The International Handbook on Computer Crime, Computer-related Economic Crime and the Infringements of Privacy, 1986, pp. 110 et seq. as well as the references in fn. 214. However, especially since the late 1980s, this situation has changed and reform legislation in the field of computer-specific procedural law is developing into the above mentioned "fifth wave" of computer-specific law reform. See the historical analysis supra chapter III.A.2.

217 See especially the European Convention on Mutual Assistance of 20 April 1959 and, with respect to the computer-specific questions discussed below, Recommendation No. R (85) 10 of the Committee of Ministers to Member States Concerning the Practical Application of the European Convention on Mutual Assistance in Criminal Matters in Respect of Letters Rogatory for the

2. The Coercive Powers of Prosecuting Authorities

a. Relevant Problems

Successful investigations in the field of information technology require a variety of information. Usually, the main object of interest is computerised data stored on corporeal data carriers. In addition, computer specific knowledge, skills and co-operation of computer specialists are necessary if the police are not familiar with the respective computer hardware or software, the security system, or its codes and passwords. In specific cases the gathering of data transferred by telecommunication lines as well as permanent registration of computer operations might be needed.

This empirical differentiation between the various types of information is essential, since the criminal procedural laws of most countries are based on express provisions of specific coercive powers. With respect to the above-mentioned requirements, most legal systems differentiate between the following issues: the possibilities to monitor publicly available facts, the powers of entry and search of premises, the powers of seizure and retention, the duty of witnesses to testify, the duty of witnesses to surrender existing means of evidence, and the powers of wiretapping.

However, in many legal systems it is questionable whether or not the traditional coercive powers are adequate for all aspects of investigations in computerised environments, since most of the traditional provisions (some of which date back to the last century) were created with respect to tangible property or traditional telephone conversations between persons, but were not especially designed for intangibles and for the special needs of a computerised information society. Only in some legal systems are there new

---

Interception of Telecommunications (adopted by the Committee of Ministers on 28 June 1985). A harmonisation of the coercive powers is especially important since a requested state can in general only provide acts which are admissible under its own law, see, e.g., Articles 3, 5 (1) (c) of the European Convention on Mutual Assistance; for Germany, Entscheidungen des Bundesgerichtshofs, Volume 7, pp. 15 et seq. at 16; for Switzerland, the Decision of the Federal Court, Official Records, Volume 98, pp. 226 et seq. at 232; *Nagel*, Beweisaufnahme im Ausland, 1988, pp. 150 et seq. For the issues of mutual assistance in the field of information technology see also Council of Europe, Report No. PC-R-CC-89-3 of 23 February 1989, pp. 70 et seq.; Dutch Committee on Computer Crime, Information Technology and Criminal Law ("Franken report"), English translation, 1987/88, pp. 91 et seq.; *Sieber*, The International Handbook on Computer Crime, Computer-related Economic Crime and the Infringements of Privacy, 1986, pp. 113 et seq. For the question of "direct access" of prosecuting agencies to foreign databases via international telecommunication networks see infra chapter III.E.2.

provisions or reform proposals concerning search and seizure of data or the duty of witnesses to produce specific computer printouts.[218]

An international comparative analysis of the relevant questions raises additional difficulties: Firstly, the various legal systems concerning investigations in criminal matters and the respective protection of civil liberties by criminal procedural law are different in many fundamental questions. Secondly, the preciseness of the legal description of coercive powers varies considerably, thus influencing the adaptability of the various legal provisions to the new challenges of the "information society". Thirdly, in many European countries it is uncertain whether or not an analogous application of the criminal procedural law *in malam partem* is possible.[219] And finally, in many countries there is still a lack of court decisions and scientific articles concerning the applicability of the traditional coercive powers in the field of information technology.

Consequently, the following chapter can only give an overview in order to initiate a more extensive international discussion. In accordance with the practical requirements of investigations in the field of information technology and based on the various coercive powers existing in most Western legal systems, it will differentiate between police surveillance on the Internet (infra b), search and seizure in automated information-systems (infra c), wiretapping of telecommunication systems and "eavesdropping" of

218 For details see the following text and references.

219 In some countries an analogous application of criminal procedural law in malam partem is generally rejected (at least in the field of coercive powers infringing civil liberties), whereas in other countries it is accepted by the prevailing opinion. See, e.g., for Austria, Decision of the High Court of Vienna, (1969) Österreichische Juristen-Zeitung/Evidenzblatt, pp. 78 et seq., at 80; *Platzgummer*, Grundzüge des österreichischen Strafverfahrens, 1984, p. 6; for Germany, Entscheidungen des Bundesverfassungsgerichts, Volume 29, pp. 183 et seq., at 196 (concerning limitations of freedom according to Articles 2 (2) and 104 (1) of the Constitution); Bär, Der Zugriff auf Computerdaten in Strafverfahren, 1992, pp. 51 et seq.; *Krey*, Parallelitäten und Divergenzen zwischen strafrechtlichem und öffentlichrechtlichem Gesetzesvorbehalt, Festschrift für Günter Blau, 1985, pp. 123 et seq., at 147 et seq.; for France, *Stefani/Levasseur/Bouloc*, Procédure Pénale, 13th ed. 1987, pp. 14 et seq.; for Switzerland, Decisions of the Federal Supreme Court, Official Records, Volume 82, pp. 234 et seq. (concerning civil procedural law); Volume 90, pp. 29 et seq.; (1976) Schweizerische Juristen-Zeitung, pp. 62 et seq. For the possibility of a delimitation of analogous interpretation (in contrast to literal application) see *Naucke*, Interpretation and Analogy in Criminal Law, Brigham Young University Law Review, 1986 Nos. 3, 535 et seq. See also in the present context *Kaspersen*, International Prosecution of Computer Crime, in: Sieber/Kaspersen/Vandenberghe/Stuurman (eds.), p. 60, distinguishing between (1) systems where the execution of coercive powers has to be stipulated explicitly in the law and (2) systems where the execution of (some) coercive powers is implicitly given, i.e. can be derived from other powers.

computers (infra d) as well as duties of active co-operation of witnesses (infra e) and of network and service providers (infra f).

b. Police Surveillance in Computer Networks ("Electronic Police Patrols")

A first question mostly unanswered by the national legislators is whether and to what extent the police can lawfully monitor computer networks. Such measures can be especially relevant when it comes to revealing and prosecuting illegal and harmful contents on the Internet. In finding a solution to this issue one has to differentiate:

Generally, the common understanding in most countries is that police officers also can act as users and in that capacity browse the net and download the information they find, like ordinary citizens do.[220] However, there are specific limits to this principle. A different evaluation holds true, e.g., if a police officer participates on the Internet under a false identity only for the purpose of obtaining evidence of a criminal offence.[221] This type of activity can be considered as "undercover activity" which should, just as any other such activity, only be engaged in if the infringement of rights of the defendant and of others is proportionate to the seriousness of the crime and the possibilities to find the evidence and the perpetrator. Under German law, e.g. participating on the Internet under a false identity could be seen as a form of undercover investigation that is only permitted under the rules and procedures set forth in Sections 110a, 110b of the German Criminal Procedural Code. A different evaluation could also be applicable if the police is inciting somebody to commit a crime. E.g., under Dutch law, a police officer would be prohibited from engaging a suspect into committing illegal acts other than the ones he already intended to commit, since it would be illegal for a law enforcement officer to actually provoke a crime.[222] In some countries, the competences for law enforcement to take action before there is a clear suspect of a criminal act – often called the pro-active stage of a criminal investigation – are enacted in special statutes. Thus, what is lawful in one country may not be lawful in another.

---

220 Cf. for Germany *Sieber*, in: Cheswick/Bellovin (eds.), Firewalls und Sicherheit im Internet, 1996, p. 304; *Bär*, Polizeilicher Zugriff auf kriminelle Mailboxen, (1995) Computer und Recht, pp. 489, 491. However, when an indication on the Internet is found, the further investigation still contains a lot of practical problems, cf. *Richard*, in: cowistra newsletter No. 6, pp. 55 et seq.

221 This is especially valid in countries in which – as for example in the Federal Republic of Germany – a "right of informational self-determination" is acknowledged. See for the right of informational self-determination e.g. *Weichert*, Informationelle Selbstbestimmung und strafrechtliche Ermittlung, 1990, especially pp. 29 et seq.

222 HR 4 December 1979, NJ 1980, 356.

Special problems arise with respect to transnational "police patrols" on the Internet. In all national legal systems analysed, there is not a clear answer to the question yet whether such activities infringe the sovereignty rights of the involved states.

c. Search and Seizure in Automated Information-Systems

Problems of Traditional Law

Search and seizure of data stored or processed in computer-systems are the most important means of obtaining evidence in computerised environments. In most cases, the relevant data can be found on movable and tangible carriers, such as tapes, magnetic or optical discs, cards, or paper listings. In other cases, the data may be permanently stored in fixed disc devices or in chips which cannot be easily removed from the computer installation. In some specific constellations (e.g. data scrolling on a screen or stored in the core-storage for only a short time), the data may not even have a permanent embodiment in a corporeal data carrier.[223]

In most countries, the traditional powers of search and entry of premises, as well as the traditional powers of seizure and retention (which are often coupled) do not pose specific problems in many cases. Collecting data stored or processed in computer-systems generally first requires entry to and search of the premises in which the computer system is installed ("powers of search and entry of premises"); it is then necessary that the data can be seized or captured ("powers of seizure and retention").

With respect to the investigation of computer data permanently stored on a corporeal data carrier, the widespread limitation of the powers of search and seizure to the search and seizure of (corporeal) "objects" relevant to the proceedings or to finding the truth[224] does not, in most countries, pose serious problems, since the right to seize and to inspect the corporeal data carrier or (in case of internal memories) the central processing unit also includes the right to copy or inspect the data.[225] In other

223 Whether in this case the rules of seizure are applicable may be doubtful, because originally they are geared to corporeal objects. Though, "searching" includes also those forms of data, if it is defined as browsing, showing data on a screen, printing or copying it onto another storage medium.

224 See, e.g., for Austria, Sections 139, 143 Criminal Procedural Code; for Belgium, Articles 36, 87 Criminal Procedural Code; for Canada, Section 487 Criminal Code; for France, Articles 56, 92-95 Criminal Procedural Code.

225 See for Germany, Bundesgerichtshof, (1988) Computer und Recht, pp. 142 et seq. (which takes this interpretation as self-evident without giving a special argument); *Leicht*, Pflicht zur

words, there should be no difference whether the data are fixed with ink on paper listings or by magnetic impulses in electronic data carriers.[226] This conclusion is even more evident for provisions in which the powers of search and/or the powers of seizure are directed towards "anything" that would be admissible as evidence at a trial.[227] The same evaluation also applies *mutatis mutandis* for the powers of confiscation.[228]

However, the application of the traditional powers of search and seizure might cause problems in the above-mentioned cases in which data are not permanently stored on a corporeal data carrier. In these instances, it is questionable whether pure data or information can be regarded as an object in the sense of criminal procedural law.[229] The same holds true if the legal principle of minimum coercion or of proportionality makes the seizure of comprehensive data carriers or complete computer installations in order to gather only a small amount of data unlawful,[230] or if the search and seizure

---

Herausgabe von Datenträgern und Mitwirkungspflichten bei der Aufbereitung von Dateien im Strafverfahren, (1986) Informatik und Recht, pp. 346 et seq., 390 et seq., at 348.

226 Another question is, whether the further evaluation of the stored data can be carried out by every police officer or only by the public prosecutor, cf. for Germany Section 110 of the Criminal Procedural Code. See also *Bär*, Durchsuchungen im EDV-Bereich II, (1995) Computer und Recht, pp. 227, 230 et seq.

227 See for Canada, Section 487 Criminal Code; for France, Article 54 Criminal Procedural Code. In other provisions, the powers of entry and search of premises are similarly not limited to searching for "objects" but also include the search and/or seizure of "objects and documents" (see for France, Article 97 Criminal Procedural Code; for Greece, Article 260 Criminal Procedural Code, of "clues" (see for Germany, Section 103 Criminal Procedural Code) or "means of evidence" (see for Germany, Section 102 Criminal Procedural Code).

228 For the provisions permitting confiscation of "objects" and/or "economic advantages" see, e.g., for Belgium, Sections 42, 43 Penal Code; for Germany, Sections 111b et seq. Criminal Procedural Code, Sections 73 et seq. Penal Code; for Norway, Sections 34-38 Penal Code. In France a new computer-specific provision of confiscation was created in the new chapter III on "Computer-Related Crime" of the Penal Code introduced by law No. 88-19 of 5 January 1988 "relative à la fraude informatique". According to the new Article 462-9 Penal Code "the court can declare the confiscation of material belonging to the convicted and having helped to commit an infraction according to the present chapter".

229 In the law of Germany and other legal systems which do not allow an analogous application of criminal procedural law (see supra chapter III, fn. 219), this question should be answered in the negative; see also *Leicht*, Pflicht zur Herausgabe von Datenträgern und Mitwirkungspflichten bei der Aufbereitung von Dateien im Strafverfahren, (1986) Informatik und Recht, pp. 346 et seq., at 348; a different result seems to be achieved by *Tschacksch*, Die strafprozessuale Editionspflicht, 1988, pp. 240 et seq. For the similar interpretation problems in the field of substantive criminal law compare *Sieber*, The International Handbook on Computer Crime, Computer-related Economic Crime and the Infringements of Privacy, pp. 53 et seq.

230 For this constellation see in Germany, Bundesgerichtshof, (1988) Computer und Recht, pp. 142 et seq. (stating the unproportionality of seizing 220 discs and the central processing unit of a computer system). In the USA see e.g. 18 U.S.C. § 2518.

of comprehensive data carriers would cause serious prejudice to business activities or to the privacy rights of third parties.[231] Uncertainties may further arise in cases in which data carriers (such as core-storage, fixed disk devices or chips) cannot be taken away to be evaluated on a police computer but must be analysed by using the computer system in question. In all these cases one might consider applying the powers of search not only for detecting a computer installation and data, but also for fixing (especially printing) the relevant data on a separate data carrier and then seizing this new object (which might be a disk or a printout).[232] However, such a construction depends on the question of whether or not and to what degree the powers of search and seizure include the power to use technical equipment and (copyrightable) programs belonging to a witness or to an accused in order to search and/or fix computer data.[233] Only some laws state that in the execution of search and seizure all "necessary measures" may be taken.[234] Consequently, in some legal systems an effective search for "pure data or information" is not provided for by the law.

---

231 This is especially the case in the field of computer communications which are particularly vulnerable to surveillance and monitoring. Search and seizure of electronic mail, telephone connections or back-up copies for example could overflow the investigators office with thousands of electronic messages and files. These data then could easily be analysed by specific programs as is already illustrated in the USA by the Computer Diagnostics Center which was developed by the Secret Service to scan the contents of electronic media seized in computer crime investigations. See *Rotenberg*, Computer Professionals for Social Responsibility, Testimony on Section 2476 The Computer Abuse Amendments Act of 1990 before The Subcommittee on Technology and Law, Committee on the Judiciary, United States Senate, 31 July 1990. In Canada Section 29 (7) Canada Evidence Act as a general rule only allows copying of records of certain financial institutions as opposed to the usual seizure of the original records.

232 See also *Harteveld*, Dwangmiddelen en computer criminaliteit, 17 (1987) Delikt en Delinquent, pp. 1042 et seq., at 1047.

233 For Germany a right to use the hardware is denied by *Leicht*, Pflicht zur Herausgabe von Datenträgern und Mitwirkungspflichten bei der Aufbereitung von Dateien im Strafverfahren, (1986) Informatik und Recht, pp. 346 et seq., at 349 and 351. For the Netherlands a right to use the hardware is assumed by *Kaspersen*, International Prosecution of Computer Crime, in: Sieber/Kaspersen/Vandenberghe/Stuurman (eds.), p. 61 on the basis of an argumentum a maiore (i.e. the right to take away the hardware) ad minus (i.e. the right to use the hardware). However, this argumentation is questionable, especially since the use of the hardware seems to be an aliud in comparison to the taking away. The same result is achieved by *Harteveld*, Dwangmiddelen en computer criminaliteit, 17 (1987) Delikt en Delinquent, pp. 1042 et seq., at 1047, who rightly justifies the use of technical equipment, but does not consider that the technical equipment might belong to another person.

234 For Japan see Articles 111, 222 (1) Criminal Procedural Code and, similarly , for France, Article 54 of the Criminal Procedural Code. In Greece the broad formulation of Articles 248, 251, 252 Criminal Procedural Code also includes the right to use hardware and software belonging to a witness or an accused.

Special problems also arise with respect to search and seizure in computer networks. A house as an object of search has physical boundaries. As far as computer networks are concerned, it is questionable whether and to what extent the right to search and seize a specific computer installation includes the right to search databases accessible by this installation but situated in other premises.[235] This question is of great practical importance since perpetrators increasingly store their data in other computer systems located elsewhere in order to hinder their prosecution. With respect to these questions, Article 125j of the Dutch Criminal Procedural Code extends Dutch search and seizure provisions by a so-called "availability"-criteria, i.e. an expansion of search and seizure from the searched premises to other computer systems but only within the limitations of the usual access rights given to the person subject to the search.

This approach might be helpful in cases of doubt. However, in general the actual powers of search and seizure must be based on a written search warrant which – in case of search and seizure of telecommunication networks – should specify the computer systems to be investigated.[236] In any case, notification requirements and other safeguards protecting the persons in question must be observed in order to prevent the search of a specific computer being used for search – or even secret surveillance – of an undefined number of other computer systems connected via telecommunication networks.[237]

Additional limits of public international law arise with respect to search and seizure of foreign databases via international telecommunication

---

235 Cf. for these powers of access in different countries the Articles in Sieber (ed.), Information Technology Crime, 1994, in particular on Germany *Möhrenschlager* (pp. 226 et seq.), on Finland *Pihlajamäki* (p. 167), on Greece *Vassilaki* (pp.246 et seq.), on UK *Wasik* (p. 502), on Hungary *Kertész/Pusztai* (p. 259), on Israel *Lederman/Shapira* (pp. 292 et seq.), on Japan *Yamaguchi* (p. 319), on Luxembourg *Jaeger* (pp. 334 et seq., 338 et seq.), on the Netherlands *Kaspersen* (pp. 367, 371), on Poland *Buchala* (p. 384), on South *Africa van der Merwe* (p. 425), on Switzerland *Roth* (p. 471), on Tunisia *Ben Halima* (pp. 479 et seq.), and on the USA *Wise* (p. 527). Also cf. in detail for the legal situation in Germany *Bär*, Der Zugriff auf Computerdaten im Strafverfahren, 1992. Cf. also Principle No. 3 of the Recommendations of the Council of Europe on criminal Procedural Law 1995: "During the execution of a search, investigating authorities should have the power, subject to appropriate safeguards, to extend the search to other computer systems within their jurisdiction which are connected by means of a network and to seize the data therein provided that immediate action is required."

236 For details of the formulation of search warrants see *Tabber*, The Computer Crime Search Warrant – A U.S. Perspective, Volume 6 Issue 1, (1990) The Computer Law and Security Report, pp. 9 et seq.

237 For wire-tapping of telecommunication systems and "eavesdropping" of computers see infra chapter III.F.2.d.

systems. In these international systems, the "direct penetration" of prosecuting authorities to foreign databases generally constitutes an infringement of the sovereignty of the state of storage (and often even a punishable offence);[238] however, there might be some specific exceptions in which "direct access" to foreign databases via telecommunication networks could be permissible[239] and the lengthy procedure of mutual assistance avoided.[240]

Problems of interpretation also arise with respect to extra safeguards for specific information. This is not only the case with the materials of professional legal advisers, doctors, journalists, and other people who are exempt from giving evidence.[241] In this area one of the latest disputes concerns the question of how far the privileges of the press should also be applicable to electronic bulletin boards.[242] Even more intricate questions arise with the application of safeguards and specific provisions to papers,

238 With respect to the punishability under the law of the accessed state, in most countries the various provisions on trade and other secrets, the anti-hacking provisions as well as special statutes (such as the Swiss Article 271 of the Penal Code on illegal acts on behalf of a foreign state) might apply. For a comparative overview of the various national trade secret provisions see *Sieber*, Legal Protection of Computer Data, Programs and Semiconductor Products, in: International Chamber of Commerce (ed.), International Contracts for Sale of Information Services, 1988, pp. 7 et seq., at 15 et seq.

239 Exceptions might be discussed especially in the following situations: (1) when the police finds a terminal showing data stored abroad, (2) when data are not protected (by security measures and legal provisions) but are freely accessible to everybody (such as public data bases), especially (3) when there is a consent of the state of storage, (4) when the prosecuting agency does not know that the data in question are stored abroad, (5) when there is a situation of urgency and only preparatory measures to preserve evidence are taken. First attempts to deal with this question can be found in Council of Europe, Computer-Related Crime, Report No. PC-R-CC-89-3 of 23 February 1989, pp. 66 et seq.; Dutch Committee on Computer Crime, Information Technology and Criminal Law ("Franken report"), English translation, 1987/88,, pp. 88 et seq.; *Kaspersen*, Strafbaarstelling van computer mis-bruik, 1990, in: Sieber/Kaspersen/Vandenberghe/Stuurman (eds.), p. 69; *Sieber*, The International Handbook on Computer Crime, 1986, p. 114. See for the situation in the USA *Perritt*, Law and the Information Superhighway, 1996, pp. 614 et seq.

240 See the references in *Sieber*, The International Emergence of Criminal Information Law, 1992, chapter IV, fn. 6.

241 See, e.g., for Canada, Section 488.1 Criminal Code; for Germany, Sections 52, 53, 97, 110 Criminal Procedural Code; for France, Articles 56-1, 57, 96, 109 Criminal Procedural Code in connection with Article 378 Penal Code; for Greece, Articles 212, 261 Criminal Procedural Code.

242 In the USA this question was especially raised in 1990 in the Neidorf-case (United States District Court Northern District of Illinois Eastern Division). See *Rotenberg*, Computer Professionals for Social Responsibility (CPSR), Testimony before the Subcommittee on Technology and Law, Committee on the Judiciary, United States Senate, 31 July 1990 (Hectography), *Bär*, Polizeilicher Zugriff auf Mailboxen, (1995) Computer und Recht, pp. 489, at 496; *Stenger*, Mailboxen – Probleme der Beweissicherung in Strafsachen, (1990) Computer und Recht, pp. 789 et seq.

documents and letters,[243] especially in the fields of electronic mail and telecommunication systems. Due to the rationale of these provisions they should generally apply in the same way to paper-based and to computer-stored material (especially to traditional mail and electronic mail); a liberal interpretation of criminal procedural law and even an analogous application of specific safeguards (in bonam partem) should be admissible.[244] In Germany the Federal Criminal Court rightly stated that the applicability of Section 110 Criminal Procedural Code, reserving for the public prosecutor the right to inspect seized "papers" (under exclusion of the police), does not depend on the information carrier used, and, consequently, includes films, magnetic tapes, discs, and the central processing unit of a computer.[245]

A more practical problem concerns the question whether seized information can be understood (e.g. if being encrypted). These problems will be discussed in the context with duties of co-operation.

Law Reform

In some countries attempts have been made to solve these uncertainties and loopholes in the field of search and seizure of data or information by legislative amendments. In the United Kingdom the general power of seizure provided by Sections 19, 20 of the Police and Criminal Evidence Act of 1984 is directed to "anything which is on the premises" and, under certain conditions, provides the power "to require any information which is contained in a computer" (for the latter duty of active co operation see infra 3).[246]

A more comprehensive attempt to address computer-related issues of criminal procedural law has been undertaken in the Netherlands in 1992:

---

243 For the wording of the various safeguards see, e.g., for Austria, Sections 145-149 Criminal Procedural Code; for Denmark, chapter 75b Sections 824-830 Administration of Justice Act; for Germany, Sections 99, 110 Criminal Procedural Code; for France, Article 97 Criminal Procedural Code; for Norway, Sections 204, 211, 212 Judicial Procedure in Criminal Cases Act of 22 May 1981; for Switzerland, Articles 66 (2), 69 Federal Criminal Procedural Code.

244 For the inadmissibility of criminal procedural law in malam partem see the references supra chapter III, fn. 219.

245 See for Germany, Bundesgerichtshof, (1988) Computer und Recht, pp. 142 et seq., at 143; Landgericht Köln, (1995) Computer und Recht, p. 419 with critical comment by *Vassilaki*; *Rengier*, Praktische Fragen bei Durchsuchungen, insbesondere in Wirtschaftsstrafsachen, (1981) Neue Zeitschrift für Strafrecht, pp. 372 et seq., at 376 et seq. For the Netherlands, Article 125l Criminal Procedural Code.

246 See for the UK, Sections 19, 20 and also Section 21 (5) of the Police and Criminal Evidence Act, Section 10 Computer Misuse Act 1990 (as amended by Section 162 Criminal Justice and Public Order Act 1994), Section 10 Finance Act, Section 63 Childrens Act.

Articles 125f et seq. Criminal Procedural Code inter alia regulate the issue of access to databases on and off the searched premise as well as the duty to assist the investigation and the handling of data gathered during the proceedings.

In 1997 Canada also amended its general provision on search and seizures in Section 487 Criminal Code to include a provision similar to the one already included before in Section 16 Competition Act.[247] The new Section 487 states that a person authorised to search a computer system may use any computer system at the building or place to search any data contained in or available to the computer system, may reproduce any data in the form of printout, may seize the printout or output for examination or coping and may use any copying equipment at the place to make copies of the data. Persons in possession and control of a place that is being searched are obliged to permit the searching officer to use the computer system for that purposes.

Such *sui generis* provisions for "gathering data" not only provide legal certainty and a basis for efficient investigations in a DP-environment, but with respect to legal policy, they can also be based on the argument that copying data is often a less severe inhibition than the seizure of data carriers. Moreover*, sui generis* provisions have the advantage that they are able to solve specific questions of "search and seizure of data", such as the recompensation of costs for the use of DP-systems, the subsequent erasure of data which are no longer required for the prosecution, or the search and seizure in telecommunication networks. Since 1989 specific regulations concerning compensation for the use of a DP-system are now provided in the German "Law on the Compensation of Witnesses and Experts".[248] With respect to the later erasure of data, Articles 125h and 125n of the Dutch Criminal Procedural Code stipulate that data of "no relevance to the investigation" shall be destroyed or erased as soon as possible.

This approach to clarify the legal situation is recommended, since effective investigations in DP-environments should be possible and based on a clear legal basis. It is true that in the future one must carefully monitor the fact that huge private data collections (especially in the field of electronic payment systems), in connection with effective powers of search and seizure, can create the danger of an intensive intrusion of the state into

247 See Section 487 (2.1.) Criminal Code, introduced by the Criminal Law Improvement Act, 1997 (see supra chapter I, fn. 21).

248 See for Germany, Section 17a of the Law on the Compensation of Witnesses and Experts, as amended by the Law on the Restructing of the Post and Telecommunication System and of the German Federal Post Organisation of 8 June 1989.

the citizens' privacy.[249] However, this danger is not primarily a problem of sui generis provisions for coercive powers of prosecuting agencies. It must be handled by adequate data protection in the private economic sector and by adequate limitations and procedural safeguards of the new sui generis provisions for search and seizure in DP-environments.

d. Wire Tapping and "Eavesdropping"

Problems of Traditional Law with Respect to Electronic Data Flow

Tapping of telecommunication lines and eavesdropping on computer systems can support criminal investigations especially in cases in which data are only transmitted and not permanently stored, in which data are merely crossing a country or in which a permanent observation of telecommunications or computer activities is necessary. However, these investigative acts not only constitute a highly efficient means of prosecution, but also a severe intrusion into the civil liberties of the tapped person. This is primarily based on the fact that the tapping of telecommunication systems and eavesdropping on computers generally is a permanent and clandestine intrusion, whereas the above-mentioned powers of entry, search and seizure usually constitute a single, "visible" interference with civil liberties. Consequently, in most countries the statutory requirements for telephone tapping and the recording of telecommunications are much higher than for other coercive measures.

However, even with respect to traditional telephone tapping the legal situation differs considerably in the various Western countries. The type of or the specific offences for which interception can legally be ordered differ. In several legal systems the principle of the inviolability of telephone communications derives from constitutional guarantees of confidentiality of correspondence and of respect for privacy;[250] in other countries the inviolability of telephone communications originates from or is established

249 See *Arzt*, Zur Beweisbeschaffungspflicht der Banken im Strafverfahren, in: Graffenried (ed.), Beiträge zum schweizerischen Bankrecht, 1987, pp. 321 et seq., at 340.

250 For the relevant guarantees in the Constitution see for Austria, Article 10; for Denmark, Article 72; for Germany, Article 10 Basic Law; for Greece, Article 19; for Japan Article 35. For Spain, Section 18 (3) of the Constitution is especially interesting in the present context because it guarantees by a wide wording the "secrecy of communications, particularly postal, telegraph and telephone communications". Similarly, for Portugal Article 34 (1) of the Constitution covers the "secrecy of correspondence and of other means of private communication". For Greece Article 19 of the Constitution establishes the "secrecy of letters and of any other free correspondence or communication".

by acts governing the administration of the telephone service[251] and/or by criminal provisions prescribing penalties for the interception of telephone communications.[252] The exceptions to the principle of inviolability of telephone communications also vary: In many Western countries there are precise legal requirements for telephone tapping (often demanded by constitutional requirements);[253] in other countries telephone tapping is based on general clauses or on an analogous application of power to intercept communications in the form of letters and telephone conversations, or it is or was even practised without any legal justification.[254] The substantive requirements for the use of telephone tapping by prosecuting agencies, as well as the requirements for control and notification, also differ considerably.[255]

---

251 See, e.g., for Germany, Section 85 Telecommunications Act of 25 July 1996 (Bundesgesetzblatt I, p. 1120).

252 See for Belgium, Section 17 of the Law on Telecommunications of 13 October 1930; for Canada, part VI, Sections 183 et seq. Criminal Code; for Denmark, Article 163 Penal Code; for Germany, Sections 201, 202a Penal Code; for Greece, Articles 249, 250, 370 A, 370 B, 370 C Criminal Code (Article 370 C was introduced by the Law No. 1805/88 of 1988 and covers any interference with data that are transported by telecommunication systems); for Italy, Section 617 Penal Code; for Norway, Article 145 Judicial Procedure in Criminal Cases Act. See also the discussion supra chapter III.B.1.c.

253 See for Austria, Article 10 of the Constitution, Sections 149a, 149b, 149c, 414a Criminal Procedural Code; for Denmark, Article 72 of the Constitution, Article 787 of the Administration of Justice Act; for Germany, Article 10 (2) Basic Law, Sections 100a, 100b Criminal Procedural Code, Sections 39, 40 Export Control Act, Section 89, 90 Telecommunications Act 1996; Section 12 Fernmeldeanlagengesetz, Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (G-10 Gesetz); for Greece, Article 19 of the Constitution and Law No. 2225 of 20 July 1994; for Italy, Articles 226-226sexies, 339 Criminal Procedural Code; for the Netherlands, Article 13 (2) of the Constitution, Articles 125f, 125g, 125h Criminal Procedural Code; for Norway, Act No. 99 of 17 December 1976 on Telephone-tapping in Connection with the Investigation of Drug Crimes, and Act No. 5 of 24 June 1915 on Supervision of Mail, Telegraphs and Telephones (concerning telephone tapping necessary for state security); for Portugal, Article 34 (1), (4) of the Constitution; for the UK, Section 2 of the Interception of Communications Act 1985.

254 In France telephone tapping is based on Article 81 Criminal Procedural Code, according to which the investigating judge, in accordance with the law, applies all informative acts which he considers helpful for finding the truth ("tous les actes d'information qu'il juge utiles à la manifestation de la vérité"). For the situation in the UK before the enactment of the Interception of Communications Act 1985 see the Malone-Decision of the European Court of Human Rights of 2 August 1984, (1985) Europäische Grundrechte Zeitschrift, pp. 17 et seq. Also Luxembourg seems to have no law expressly permitting wiretapping. For the relevant requirements to the respective statutory powers compare *Noll*, Technische Methoden zur Überwachung verdächtiger Personen im Strafverfahren, 91 (1975) Schweizerische Zeitschrift für Strafrecht, pp. 44 et seq., at 49 et seq.

255 In most countries the use of telephone tapping is restricted to the investigation of serious crimes (which are defined either by the number of years' of imprisonment possible, by general clauses, or by enumerating specific actions giving grounds for telephone tapping). In some countries, however, computer-related crimes are not part of these crimes. See, e.g. for Greece, Article 4 Law

Consequently, the question as to whether or not the traditional powers of wiretapping can be applied to tapping other telecommunication services and computer systems was answered differently in various countries. However, in the meantime, most countries seem to have arrived at the point that interception powers concern not only voice telephony, but include all forms of modern telecommunication traffic, as for example fax or other data communication. No computer-specific issues arise in legal systems in which the statutory law permits, e.g., the "surveillance of the telecommunication traffic including the recording of its content".[256] On the other hand, computer specific problems of interpretation exist especially in countries which only permit the "monitoring of conversations"[257] or the "surveillance and tapping of the telecommunication traffic on sound carriers".[258] Such clauses are particularly problematic if an analogous application of coercive powers in criminal procedural law is not accepted.[259] This was illustrated in the Netherlands, where the judicial authorities wanted to intercept telex communication by analogy with the old Articles 125f et seq. of the Dutch Criminal Procedural Code; however, the postal

No. 2225/1994, for the UK Section 2 (a) of the Interception of Communications Act 1985. Canada is currently considering amending its Criminal Code to also include computer crimes in the respective catalogue of Section 183 Criminal Code (see the Criminal Law Improvement Act, 1997, supra chapter I, fn. 21).Under most legislations telephone tapping is an exceptional means of investigation and subject to one or more additional conditions (in particular there must be a specific degree of suspicion of an offence, monitoring must be crucial to the inquiry, traditional methods of inquiry must be impractical or must have failed). Generally, telephone tapping requires judicial authorisation (by a judge or by a public prosecutor); only in a few cases is the use of tapping decided by the administrative authority. Finally, there are legal systems which consider any telephone tapping illegal. For a comparative overview see Council of Europe, Legislative Dossier No. 2, Telephone Tapping and the Recording of Telecommunications in some Council of Europe Member States, Strasbourg, May 1982; Eser/Huber (eds.) Strafrechtsentwicklung in Europa, 1985, pp. 479 (Italy), 516, 528 (Netherlands), 588 (Poland), 690 (Sweden), 713 et seq., 750 et seq. (Switzerland). For the legal basis of telephone tapping practiced by German and US-American intelligence agencies for preventive aims see *Beier*, Geheime Überwachungsmaßnahmen zu Staatssicherheitszwecken außerhalb des Gesetzes zur Beschränkung von Artikel 10 GG (G 10), 1988.

256 See for Austria, Section 149a Criminal Procedural Code; for the Netherlands, Articles 125f, 125g Criminal Procedural Code. Also compare for the UK Section 2 (1) of the Interception of Communications 1985 Act of ("to intercept, in the course of their transmission by post or by means of public telecommunication system, such communications as are described in the warrant").

257 See for Sweden, chapter 27 Section 16 of the Criminal Procedural Code.

258 See for Germany, Section 100a Criminal Procedural Code (prior to 1989). In Canada in part VI of the Criminal Code, which provides a scheme for interception, "private communication" applies also to computer communication on a network, be it private or public communication network, if the communication is between persons.

259 See the references supra chapter III, fn. 219.

administration refused to co-operate, invoking the exact wording of the law referring to "telephone conversations".[260] This rule of interpretation of criminal procedural law is in accordance with a decision of the Swiss Federal Supreme Court, which in 1975 refused to justify cantonal telephone tapping by an analogous application of Article 104 of the Criminal Procedural Code of the Canton of Zurich which only permitted the control of letters, telegrams and other consignments.[261] Some countries may apply provisions on warrants if computer communication is concerned that is not already covered by provisions on the interception of "private communication".[262] Other countries – such as Japan – have no provision at all which might be applicable.

Additional Problems with Respect to Stored Mail

Additional problems with respect to wiretapping of computer communications arise if computer data is not only transmitted (as in the case of Internet relay chat) but also stored permanently (as in the case of e-mail). In this cases it is clear that the (clandestine) interception of the *transmitted data flow* is only possible under the severe requirements of wiretaps statutes. However, uncertainties exist with respect to the *data stored* e.g. in the addresses mail box containing the incoming mail. In most legal systems it is unclear whether this stored mail data can be accessed under the more generous provisions of search and seizure. Furthermore it is an open question whether a clandestine evaluation of this stored data is possible under the wiretapping rules or if such a clandestine evaluation would constitute an act of "state hacking" (comparable to illegal eavesdropping) not permitted by criminal procedural law in many countries.

These questions could be solved either by a more technical or a more functional approach. In a more technical approach, one could separate the transmission and the storage functions, thus enabling the search and seizure of stored e-mail (i.e. of the hard disc the e-mail is stored on). In a functional approach, one could regard the storage function as a part of an entire communication process and apply the provisions of wiretapping to the whole process including the stored data. However, the latter approach, even though demanding higher requirements for accessing the stored mail, would

260 See for the Netherlands, Dutch Committee on Computer Crime, Information Technology and Criminal Law ("Franken report"), English translation, 1987/88, p. 73. For the revised wording of Articles 125f et seq. Dutch Criminal Procedural Code see supra III.E.2.c.

261 See Decision of the Federal Court, (1976) Schweizerische Juristen-Zeitung, pp. 62 et seq.

262 See, e.g., for Canada, Section 487.01 Criminal Code if Part VI Criminal Code is not applicable.

create the danger that the wiretap statutes (originally applied outside the concerned persons premises) would be transformed to powers of (eventually clandestine) hacking of mail servers comparable to eavesdropping, not permitted by criminal procedural law in many countries.

In Germany (where the interception of all modern forms of communication is possible under the revised paragraphs of the Criminal Procedural Code) an investigating judge of the Bundesgerichtshof has taken the position that direct access to a remote computer system can be granted to law-enforcement by utilising the rules on interception of telecommunication. However, this interception was limited in analogy to house searches to one single access of the system. Any further need for monitoring the traffic to and from such a system would have to follow the rules of wiretapping. The decision received harsh criticism by academic literature.[263]

Law Reform

In order to avoid problems of interpretation, most countries have already enacted or proposed new legislation making it possible to tap all kinds of telecommunication under the same conditions as the tapping of telephone conversations. In Denmark in 1985 a new provision of the Administration of Justice Act was passed according to which the police, under certain conditions, may "interfere in private communication by ... tapping telephone conversations or other similar telecommunication".[264] In 1986 the USA's Electronic Communications Privacy Act extended the legal protection and the powers of wire tapping from oral communication (covered by the Omnibus Crime Control and Save Street Act of 1968) to "electronic communication".[265] Similarly, in the Federal Republic of Germany an amendment to the Criminal Procedural Code extended the possibilities of wiretapping to public telecommunication networks in 1989.[266] In 1993,

263 Cf. Bundesgerichtshof, (1996) Computer und Recht, p. 488. To this decision see *Bär*, (1996) Computer und Recht, p. 490 and *Palm/Roy,* (1997) Neue Juristische Wochenschrift, p. 1904.

264 Chapter 71, Section 780 of the Administration of Justice Act (amended by Act No. 227 of 6 June 1985).

265 The 1986 Electronic Communications Privacy Act (18 U.S.C. § 2510 (12)) defines "electronic communication" as "any transfer of signs, signals, writings, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectric or photooptical system that affects interstate or foreign commerce." See also the Digital Telephony Act of 1994 (18 U.S.C. §§ 2601-2608).

266 Article 4 (17s) of the "Poststrukturgesetz" of 14 June 1989, amending Sections 100a, 100b of the Criminal Procedural Code. At the moment, a bill (Begleitgesetz zum Telekommunikationsgesetz, Bundestagsdrucksache 13/8016 of 23 June 1997) plans to amend the relevant wiretapping

Austria amended its laws on wiretapping making it clear that "surveillance" refers not only to wiretapping of content of a conversation but also to the circumstances of such a conversation such as its duration or location. Also surveillance is not limited to the transmission of speech but covers all forms of telecommunication. Articles 125f-h of the Dutch Criminal Procedural Code have eliminated many problems by extending the scope of Dutch wiretapping rules to any form of communication via telecommunication networks.[267]

The problem of extending the list of offences for which wiretapping is possible was taken up in Canada. In 1997, the Criminal Law Improvement Act extended the list of offences to include the following Sections of the Criminal Codes: Section 327 (possession of a device to obtain the use of a telecommunication facility or service), Section 341 (unauthorised use of a computer), and Section 342.2 (possession of a device to obtain a computer service).

With respect to future policy making further clarifications are to be recommended since telecommunication between computers does not merit more protection than telecommunication between persons. However, the respective coercive powers should be worded precisely and should especially exclude the danger of (ab)using the powers of wiretapping telecommunication between computer systems for general eavesdropping on (or bugging of) personal communication.[268] In addition, exact definitions, what systems should be seen as public networks, are necessary.

---

provisions in order to give them a broader applicability that covers every "commercial provision of telecommunications services".

267 Additional rules on wiretapping in the Netherlands can be found in Articles 64, 64a Telecommunications Act and the Decree on Tapping Mobile Telecommunication GSM. Similarly, the Scottish Law Commission recommended a new provision, similar to the one contained in the Interception of Communications Act 1985, in order to obtain remote, and therefore clandestine, access to a program or data stored in a computer: The Law Commission specified that the grounds upon which authorisation may be granted should be the same as in Section 2 (2) of the Interception of Communications Act 1985, namely that it is necessary (a) in the interests of national security, (b) for the purpose of preventing or detecting serious crime, or (c) for the purpose of safeguarding the economic well-being of the UK. See Scottish Law Commission, Report on Computer Crime, Her Majesty's Stationery Office, 1987, pp. 21 et seq., 29 et seq. concerning Section 2 of the Draft Computer Crime Bill (Scotland); *Wasik*, The Computer Misuse Act 1990, (1990) The Criminal Law Review, pp. 767 et seq., at 775 et seq.

268 In many countries eavesdropping on personal communication is not a legal means for the repressive prosecution of crimes, but is reserved for the preventive activity of intelligence agencies. See the references supra chapter III.F.2.d. For a different solution with respect to specific crimes see Section 100c (1) No. 2 of the German Criminal Procedural Law. For the respective questions of legal policy see *Noll*, Technische Methoden zur Überwachung verdächtiger Personen im Strafverfahren, 91 (1975) Schweizerische Zeitschrift für Strafrecht, pp. 44 et seq., at

e. Duties of Active Co-operation of Witnesses

The Practical Problems

The aforementioned powers of entry, search and seizure, wiretapping and even a *sui generis* power of gathering data do not guarantee a successful investigation in many cases since the traditional authorities often lack the skills necessary to access modern data processing systems. Authorities are often without the required knowledge about computer hardware, operating systems and standard software. These problems can be solved by a better training of investigation officers.[269] However, access to computer systems is also faced with specific problems originating from the complex nature of modern information technology which can only partially be solved by better police training. This is mainly the case with respect to specific security software and encryption designed for the prevention of unauthorised access to information.[270] Serious problems are also caused by the multitude of data stored in computer systems and by the limited time and the limited financial resources of prosecuting authorities for checking these data. Consequently, the duties of citizens in co-operating with prosecuting agencies become of much greater importance in computerised environments than they are in a non-technical "visible" area.

As far as search and seizure is concerned, the traditional legal systems of most Western countries include two instruments which might be used to reach the necessary co-operation in order to gather evidence in a computerised environment: the duty to surrender sizeable objects of evidence and the duty to testify. In some countries additional and further-reaching provisions or reform proposals have been enacted or suggested. But also in the field of wiretapping, there are some needs of active co-operation.

---

71 et seq. For the relevant work of international organisations in this context see infra chapter IV.E.

269 See Council of Europe, Teaching, Research and Training in the Field of "Computer and Law", Recommendation No. R (80) 3 adopted by the Committee of Ministers of the Council of Europe on 30 April 1980 and Explanatory Memorandum, 1981.

270 In many countries at present a public "crypto"-debate is being held. There is certainly a need for intelligence services and law enforcement authorities that telecommunication for criminal purposes remains interceptable and understandable to its interceptors; on the other hand business organisations and private persons have a legitimate interest in applying encryption in their communications. See infra III.F.2.b and IV.F.2.b.

Duties to Surrender Seizeable Objects

The duty to surrender sizeable objects is often coupled with the powers of search and seizure. In many countries the holder of a sizeable object is obliged to deliver it on request to the (judicial) authorities;[271] however, some legal systems do not provide for such an obligation, and in some countries the respective court orders are not enforceable.[272] The duty to surrender sizeable objects can help the investigation authorities especially in selecting specific data carriers among the many tapes and disks which are usually stored in a computer centre. However, the obligation to surrender sizeable objects generally does not include the duty to print or deliver specific information stored on a data carrier, since in most countries the respective legal obligations are directed to corporeal objects and, in general, the duty to surrender does not go further than the powers of seizure (also with respect to privileges of witnesses).[273] Consequently, the duty to surrender only covers existing (corporeal) objects.[274] An analogous application of these provisions permitting the production of specific information or the recognition of a respective uncodified "citizen's duty"[275] seems doubtful, since the exclusive enumeration of specific coercive powers in criminal procedural law is an essential principle in the protection of civil liberties. The same holds true for an analogous application of the duties to produce computer data according to tax and company law.[276] Consequently, in many countries the powers of seizure and the duties to surrender sizeable objects

271 See for Austria, Section 143 (2) Criminal Procedural Code; for Germany, Sections 95 (1), 70 Criminal Procedural Code.

272 See, e.g., the legal situation in Belgium or France. For a comparative overview compare *Arzt*, Zur Beweisbeschaffungspflicht der Banken im Strafverfahren, in: Graffenried (ed.), p. 326.

273 See *Arzt*, Zur Beweisbeschaffungspflicht der Banken im Strafverfahren, in: Graffenried (ed.), p. 328; *Leicht*, Pflicht zur Herausgabe von Datenträgern und Mitwirkungspflichten bei der Aufbereitung von Dateien im Strafverfahren, (1986) Informatik und Recht, pp. 346 et seq., at 351; *Tschacksch*, Die strafprozessuale Editionspflicht, 1988, pp. 29 et seq. (however, in contradiction to pp. 241 et seq., where the limitation of Sections 94, 95 Criminal Procedural Code to "corporeal objects" is not taken into account).

274 See *Arzt*, Zur Beweisbeschaffungspflicht der Banken im Strafverfahren, in: Graffenried (ed.), p. 329.

275 For the rejection of such a citizen's duty to co-operate ("staatsbürgerliche Mitwirkungspflicht") in the law of Germany see *Nelles*, Strafprozeßrecht: Spuren aus der Datensammlung, (1987) Juristische Schulung, pp. 51 et seq., at 53.

276 In Germany, Sections 261 Commercial Code, 97 (3) cl. 2, 147 (5) Tax Code, 85 Code of Procedure for Fiscal Courts are not applicable in the field of criminal procedural law; see *Leicht*, Pflicht zur Herausgabe von Datenträgern und Mitwirkungspflichten bei der Aufbereitung von Dateien im Strafverfahren, (1986) Informatik und Recht, pp. 346 et seq., at 351 et seq.; *Nelles*, Strafprozeßrecht: Spuren aus der Datensammlung, (1987) Juristische Schulung, pp. 51 et seq., at 53; *Tschacksch*, Die strafprozessuale Editionspflicht, 1988, pp. 251 et seq.

can only support "voluntary" printing of specific information. The German practice with respect to search and seizure in the field of banking shows that banks often voluntarily print out specific data in order to prevent the seizure of large volumes of data carriers.[277] However, the threat of a comprehensive seizure and serious prejudice to business activities cannot be regarded as a satisfactory legal solution for the relevant problems.

Duties to Testify

In many cases an important duty of active co-operation can be based on the duties to testify, i.e. the duty of (unsuspected) witnesses to "testify", "to tell the truth", "to answer questions", et al.[278] This is especially the case in countries in which the traditional duties to testify contain the further-reaching obligation of the witness "to refresh his knowledge of the case, e.g. by examining account books, letters, documents, and objects that are available to the said witness without special inconvenience, and to make notes and bring them along to the court".[279] These duties to testify can be used successfully for example to find out a specific password necessary to access a computer system or to locate specific information in large data storages: In theory, it is possible to seize a computer system – in order to investigate its content, but in practise this will not help when the access to the system is logically secured. To a certain extent it might also be possible to use a series and/or combination of questions to gain explanations on the functioning of a difficult security system. However, in most legal systems

277 In Germany this procedure is disputed especially with respect to the compensation of costs. See Decision of the *Federal Criminal Court (BGH)*, (1982) Neue Zeitschrift für Strafrecht (NStZ), pp. 118 et seq.; Decision of the *High Court of Bremen*, (1976) Neue Juristische Wochenschrift (NJW), pp. 685 et seq.; *Sannwald*, Entschädigungsansprüche von Kreditinstituten gegenüber auskunftsersuchenden Ermittlungsbehörden, (1984) Neue Juristische Wochenschrift (NJW), pp. 2495 et seq; *Tschacksch*, Die strafprozessuale Editionspflicht, 1988, pp. 293 et seq., 342 et seq.

278 See for Austria, Sections 150-53 Criminal Procedural Code; for Belgium, Articles 71, 86 Criminal Procedural Code; for Canada, Sections 698 et seq. Criminal Code; for Denmark, chapter 18, Sections 168-190 Administration of Justice Act; for Germany, Sections 57, 69, 70 Criminal Procedural Code; for France, Articles 109, 331, 437, 438 Criminal Procedural Code; for Greece, Article 209 Criminal Procedural Code; for Japan, Article 226 Criminal Procedural Code; for Norway, Sections 117-125 Criminal Procedural Code.

279 See for Norway, Section 116 of the Criminal Procedural Code. Also for Canada, Sections 698-700 Criminal Code. Some legal systems consider such a duty to be implied in the duty to testify: See, e.g., for Germany, Entscheidungen des Reichsgerichts, Volume 62, pp. 126 et seq., Bundesgerichtshof, (1973) Goltdammer's Archiv für Strafrecht, pp. 376 et seq.; *Tschacksch*, Die strafprozessuale Editionspflicht, 1988, pp. 37 et seq. In other countries the preparatory duties of witnesses are more limited: See, e.g., for Switzerland, *Arzt*, Zur Beweisbeschaffungspflicht der Banken im Strafverfahren, in: Graffenried (ed.), p. 323.

the traditional duties to testify cannot be extended to efficient duties of co-operation, especially not to printing out specific information.[280] The main reason for this conclusion is the fact that the duty to testify – and consequently the duty of witnesses to refresh their knowledge – refers only to knowledge which the witness already had in his mind and not to new information.[281] A different conclusion would also confuse the roles of witnesses and experts. Furthermore, in many countries the witness must testify before a judge (and in some countries to the public prosecutor), but not before police conducting the investigation in practice;[282] in some legal systems the duties to testify exist only in a later stage of the proceedings and not during the police investigation. Moreover, the requirement of a (written or an oral) court summons to be given to the witness in due time could make such proceedings ineffective.[283]

Law Reform and Evaluation

In order to make investigations in computerised environments more efficient, some countries have enacted or suggested new compulsory duties to produce specific information. According to the Police and Criminal Evidence Act 1984 of the United Kingdom the constable "may require any information which is contained in a computer and is accessible from the premises to be produced in a form in which it can be taken away and in which it is visible and legible".[284] In Canada the Mutual Legal Assistance Act provides for an evidence gathering order addressed to a person "to make a copy of a record or to make a record from data and to bring the copy or record with him".[285]

---

280 See also *Leicht*, Pflicht zur Herausgabe von Datenträgern und Mitwirkungspflichten bei der Aufbereitung von Dateien im Strafverfahren, (1986) Informatik und Recht, pp. 346 et seq., at 354, 390 et seq., 392.

281 See for Germany, Decision of the Oberlandesgericht Köln, (1973) Neue Juristische Wochenschrift, pp. 1983 et seq.; *Engisch*, Die Verletzung der Erkundigungspflicht, 52 (1932) Zeitschrift für die gesamte Strafrechtswissenschaft, pp. 661 et seq.; for Switzerland, *Arzt*, Zur Beweisbeschaffungspflicht der Banken im Strafverfahren, in: Graffenried (ed.), p. 324.

282 See, e.g., the legal situation in Germany (no duty to testify to the police) in contrast to the legal situation in Italy. For references of the duties to testify see supra chapter III, fn. 256.

283 See for Germany, *Leicht*, Pflicht zur Herausgabe von Datenträgern und Mitwirkungspflichten bei der Aufbereitung von Dateien im Strafverfahren, (1986) Informatik und Recht, pp. 390 et seq., at 391 et seq.; *Rengier*, Praktische Fragen bei Durchsuchungen, insbesondere in Wirtschaftsstrafsachen, (1981) Neue Zeitschrift für Strafrecht, pp. 372 et seq., at 376.

284 See for the UK, Sections 19 (4), 20 (1) Police and Criminal Evidence Act.

285 See for Canada, Section 18 (2) Mutual Legal Assistance in Criminal Matters Act, S.C. 1988, c. 37, in force since 1 October 1988. Section 2 (1) defines "data" as "representations, in any form, of

The Dutch Criminal Procedural Code provides for comprehensive and far-reaching active duties of witnesses to assist law-enforcement in their effort to search and seize data stored on computer systems. Article 125i Criminal Procedural Code states that anyone who can reasonably be expected to have access to the relevant data has a legal obligation to produce this data in a way the court sees fit. Under Article 125k Criminal Procedural Code a person can be ordered to provide access to data by using decryption tools available to the person or by helping the police break the security systems of a computer.[286]

However, with respect to data accessible via international telecommunication networks, all of these provisions leave the question open whether and to what degree a state, in accordance with international public law, has the right to oblige its citizens to gather evidence in foreign countries.[287] Furthermore, it is unclear under which conditions the citizens have the right to deny co-operation.

The question whether or not such duties to produce and hand over computer printouts should be recommended *de lege ferenda* therefore requires a differentiation between the duties of witnesses and the duties of defendants or suspected persons. With respect to (unsuspected) witnesses there are good arguments for the introduction of such a duty.[288] First, the duty to print out specific information also exists in tax and company law and is not a too intensive intrusion of the state into the citizen's rights, especially with respect to the aim of finding the truth in criminal proceedings.[289] Secondly, the duty to print out specific information is often less infringing to the citizen's rights than a comprehensive search of a company and seizure of data carriers (which can often bring the operations of the company in question to a complete standstill and jeopardise valuable information). Thirdly, in many cases a duty to print out computer-stored evidence can be of essential significance for criminal proceedings. However,

---

information or concepts" as well as "record" as "any material on which data are recorded or marked and which is capable of being read or understood by a person or a computer system or other device".

286 In the UK the newly elected Labour-government has put forward similar proposals. See <http://www.labour.org.uk/views/info-highway/content.html> (accessed on 21 January 1998).

287 See *Sieber*, Transnational Enterprises and Criminal Law, in: Tiedemann (ed.), Multinationale Unternehmen und Strafrecht, 1980, pp. 155 et seq., at 170 et seq. Also compare the references for the similar question dealt with in chapter III.E.2.c.

288 For the same result see *Kaspersen*, International Prosecution of Computer Crime, in: Sieber/Kaspersen/Vandenberghe/Stuurman (eds.), p. 65.

289 For the justification and the limits of duties of active co-operation in these areas of law see *Eilers*, Das Steuergeheimnis als Grenze des internationalen Auskunftsverkehrs, 1987, pp. 47 et seq.

the evaluation and recommendation of such a duty of active co-operation presupposes that the traditional rights to refuse to testify apply *mutatis mutandis*, that the witnesses are financially compensated for their efforts, and that special respect is given to the range of this duty in international telecommunication networks.

On the other hand, with respect to the defendant or suspect, a duty of active co-operation should be decisively rejected since this duty could impede the accused's right to remain silent and infringe the fundamental principle that the defendant does not have to incriminate himself. It is true that the wording of Article 14 (3) g of the International Covenant on Civil and Political Rights of 1966 only guarantees that, in the determination of any criminal charge against him, everyone shall be entitled to the "minimum guarantee" of "not to be compelled to testify against himself or to confess guilt".[290] Similarly, the fifth amendment to the Constitution of the USA – and similarly part 1 Section 11 (c) of the Canadian Constitution of 1981 – declares that "no person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury ... nor shall be compelled in any criminal case to be a witness against himself". Specific guarantees in the criminal procedural law of other countries are also limited to oral testimony.[291] The reasons underlying these guarantees justify and demand a general privilege against any active self-incrimination.[292] Consequently, the right of the accused not to testify against himself – and similarly all other procedural exemptions to testify – should apply mutadis mutandis to the duty to produce computer data and to any duty of active co-operation.[293]

---

290 International Covenant on Civil and Political Rights, Adopted by General Assembly Resolution 2200 A (XXI) of 16 December 1966, published in Official Records of the Twenty-first Session of the General Assembly, Supplement No. 16 (A/6316) 52.

291 See for Germany, Section 55 (and furthermore Section 136 (1)) of the Criminal Procedural Code: "Every witness has the right to refuse to answer to such questions which would subject him or one of his relatives mentioned in Section 52 (1) to the danger of criminal or regulatory prosecution." A similar provision constitutes, e.g., for Greece, Article 223 Section 2 Criminal Procedural Code.

292 See for Germany, Entscheidungen des Bundesverfassungsgerichts, Volume 56, pp. 37 et seq.; *Reiß*, Besteuerungsverfahren und Strafverfahren, 1987, pp. 140 et seq.; *Rogall*, Der Beschuldigte als Beweismittel gegen sich selbst, 1977; for Switzerland, *Arzt*, Zur Beweisbeschaffungspflicht der Banken im Strafverfahren, in: Graffenried (ed.), p. 327; for the UK, *Zuckerman*, Trial by Unfair Means – The Report of the Working Group on the Right of Silence, (1989) The Criminal Law Review, pp. 855 et seq. Nevertheless, in the Netherlands the introduction of such a duty of the accused was seriously disputed.

293 Specifically excluding the suspect from any duty to actively co-operate, e.g., Article 125m (1) Dutch Criminal Procedural Code.

f. Special Duties of Active Co-operation with Respect to Wiretapping

A successful interception of telecommunication services requires a co-operation between the law enforcement authorities and the network and service providers: First of all, the provider of a telecommunication system to be intercepted must in general be required to make interception possible. Then it is necessary to provide the relevant customer data (especially names, addresses, and numbers). Additional, co-operation is needed to obtain the so-called traffic data, i.e. data about a the time of a communication, its duration, the involved subscriber-numbers and so on.[294] Furthermore, the understanding of the intercepted data requires knowledge of the particular application program. All these questions and the duty of co-operation of service providers have become especially crucial due to the privatisation of telecommunication services in recent years.

As a consequence, in some countries new special duties of network and service providers with respect to the interception of telecommunications have been created. Often, the new provisions were not included in the criminal procedural codes but in specific telecommunication legislation. E.g. in Germany, the new Telecommunications Act of 1996 contains precise provisions with respect to the duties of (now: private) network and service providers to supply customer data for prosecuting agencies, to install technical interfaces for wiretapping, to execute judicial wiretap orders and not to disclose running wiretap operations.[295] In the age of privately owned telecommunication networks, such precise duties are necessary in order to make judicial wiretap orders executable.[296]

3. Specific Problems with Personal Data

The coercive powers of collecting evidence in the field of information technology analysed cover both personal and non personal data. However, with respect to personal data there are additional legal problems which mainly concern the gathering, storing and linking of personal data in the course of criminal proceedings. In this field of "privacy protection in criminal

294 For example Section 492.2 of the Canadian Criminal Code provides for the issuance of a judicial warrant to install, maintain, remove and monitor a "number recorder" for the purpose of recording or identifying the telephone number or location of the telephone from which a call originates.

295 See Sections 90, 92 Telekommunikationsgesetz of 1 August 1996, Bundesgesetzblatt I, 1996, pp. 1117 et seq.

296 For details see *Sieber*, in: Bayerisches Staatsministerium für Unterricht, Kultus, Wissenschaft und Kunst (ed.), Hochschulnetze in Bayern, 1997, pp. 115 et seq.

matters" the legal requirements vary considerably in Western countries.[297] The differences between the various legal systems are not only differences in substantive law requirements, but also concern the constitutional background, the legal context and the legislative technique of the relevant provisions. Special problems with data protection appear, when personal data are transferred form one country to another.[298]

a. Constitutional Requirements

An extensive discussion of the underlying constitutional requirements for gathering, storing and linking personal data exists only in few countries. For example, in the Federal Republic of Germany, the Bundesverfassungsgericht recognised in its famous "Census-Decision" that the state's storage of personal data (especially in computer systems) could influence the citizens' behaviour and endanger their general liberty of action, and must therefore be considered as a violation of civil liberties ("right of informational self-determination"[299]) requiring an express and precise legal basis; this legal basis must balance the interests of the individual and his right to privacy on the one hand and the interests of society in the suppression of criminal offences and the maintenance of public order on the other hand.[300] The new Spanish Constitution of 1978,[301] the new revised Portuguese Constitution of 1982, the Dutch Constitution of 1983 and the new Brazilian Constitution of

297 For the respective proposals of international organisation see infra chapter IV.E.

298 Cf. for the comparable transmission between tax offices *Carl/Klos*, Internationale Kontrollmitteilungen zwischen Steuerbehörden, (1995) Computer und Recht, pp. 235 et seq.

299 Cf. for the right of informational self-determination in criminal procedural law *Weichert*, Informationelle Selbstbestimmung und strafrechtliche Ermittlung, 1990. For the consequences for the treatment of personal data especially at pp. 114 et seq. For the constitutional problems of "strategic wire tapping" (i.e. without any concrete suspicion) Bundesverfassungsgericht, (1996) Neue Juristische Wochenschrift, p. 114.

300 Entscheidungen des Bundesverfassungsgerichts, Volume 65, pp. 1 et seq. ("Census-Decision") and Volume 67, pp. 100 et seq. ("Flick-Decision"). For the underlying constitutional law questions see *Häberle*, Die Wesensgehaltsgarantie des Artikel 19 II GG, 3rd ed. 1983, pp. 335 et seq.*; Schmitt Glaeser*, Schutz der Privatsphäre, in: Isensee/Kirchhof (eds.), Handbuch des Staatsrechts, 6th ed. 1989, Section 129, Nos. 76 et seq.; *Scholz/Pitschas*, Informationelle Selbstbestimmung und staatliche Informationsverantwortung, 1984; *Vogelgesang*, Grundrecht auf informationelle Selbstbestimmung, 1987. For the consequences in the field of criminal procedural law compare *Rogall*, Moderne Fahndungsmethoden im Lichte gewandelten Grundrechtsverständnisses, (1985) Goltdammer's Archiv für Strafrecht, pp. 1 et seq.; *Wolter*, Heimliche und automatisierte Informationseingriffe in den Datengrundrechtsschutz, (1988) Goltdammer's Archiv für Strafrecht (GA), pp. 57 et seq., 129 et seq.

301 See for Spain, Article 18 (4) of the Constitution of 1978: "The law shall limit the use of information, to guarantee personal and family honor, the privacy of citizens and the full exercise of their rights." For the relevant criminal law problems cf. *Morales*, Problemática jurídico-penal de las libertades informáticas en España tras diez años de vigencia de la Constitución de 1978, 1989.

1988 even contain specific safeguards protecting the citizens' privacy against the risk of modern computer technology.[302] On the other hand, in many other countries such as Denmark, France or Switzerland, the gathering and storing of personal data is not (yet) considered to be of constitutional relevance, but is only dealt with by the legislature in ordinary statutory (non-constitutional) law on a "voluntary basis".[303]

b. Legal Regulations

The various legal systems' regulating the legality of gathering, storing and linking of personal data (either on a constitutional "compulsory" or on an ordinary "voluntary" legal basis) place the relevant provisions in different contexts and laws. A few countries, such as Germany, placed most of the respective provisions within the purview of their criminal procedural law.[304] This legislative technique has the advantage that the criminal procedural code upholds its monopoly in the application of criminal law and thus remains the exclusive enumeration for any infringement of civil liberties in the course of criminal prosecution. However, most countries (uniquely or in part) regulate the legality of police files in their general data protection acts; in the majority of cases the relevant provisions are applicable both to the repressive activity of the police (prosecution of crimes) and to its preventive action (maintenance of public order).[305] Some countries exclude police files –

302 See, e.g., for Portugal, Article 35 ("Use of data processing") of the revised Constitution of 1982: "1. All citizens shall have the right to information on the contents of data bases concerning them and on the use for which it is intended. They shall be entitled to require the said contents to be corrected and brought up to date. 2. Data processing shall not be used for information concerning a person's political convictions, religious beliefs or private life except in the case of non-identifiable data for statistical purposes. 3. Citizens shall not be given all-purpose national identification numbers."

303 See, e.g., for France, Article 26 of the "loi relative à l'informatique, aux fichiers et aux libertés" and *Poullet*, Le fondement du droit à la protection des données nominatives: propriété ou libertés, Congress Proceedings, Montreal 1989. For a comparative study of the constitutional law of Germany and the USA cf. *Schwartz*, The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination, 37 (1989) The American Journal of Comparative Law, pp. 675 et seq.

304 In Germany the Draft of a Draft of a Criminal Procedural Code Amendment Act, Bundesratsdrucksache 961/96 of 20 December 1996) includes new provisions on data processing and the use of personal-related information in criminal procedures. At present, the gathering, storing and linking of personal data in the course of criminal proceedings in Germany is only governed by Sections 98a, 98b, 98c (computer matching), Section 163d Criminal Procedural Code (specific computer matching) and by the general Data Protection Law (see supra chapter I, fn. 19). In France Articles 768 et seq. of the Criminal Procedural Code contain specific provisions on the automated national register.

305 In Austria the use of personal data for criminal investigations is regulated by the Data Protection Act; data processing is legal as far as it is an essential prerequisite for fulfilling tasks provided for

completely or partly – from their general data protection laws and/or create specific acts or decrees for all types of (repressive or preventive) police data.[306] In a number of countries additional specific acts concerning criminal records exist.[307] However, there are also legal systems without any legal provisions (enacted by Parliament) regulating the general use of personal data in the police sector.

Apart from these questions of placement and context of the relevant statutes, the legislative technique, the content, and the control mechanisms of the relevant laws also vary. With respect to the legislative technique some countries such as Germany, consider a more detailed and precise regulation necessary; other countries resort to more or less general clauses.

As far as the contents of the various laws are concerned serious limitations seem to be rarely applicable to police files. Far-reaching and precise regulations on the deletion of entries exist only with respect to registers of criminal convictions.[308]

4. Admissibility of Computer-Generated Evidence

The admissibility of computer-generated evidence is not only important for the use of computer records in criminal trial process, but is also essential for defining the extent of the above-described coercive powers and of mutual assistance, since in most countries coercive powers are only applicable to material that would be admissible in evidence at a trial; consequently, if specific computer data or printouts could not be used as evidence, they could also not be searched and seized. In practice the various legal problems are particularly crucial since computer printouts and computer

in the law (Sections 6 and 7 of the Act). In Canada the Federal Privacy Act (R.S.C. 1985, c. P-21) governs the collection, retention and use of personal information by federal institutions including the Royal Canadian Mounted Police; data processing of provincial police forces is regulated, e.g., in the Ontario Freedom of Information and Protection of Privacy Act (S.O. 1987, c. 25; especially Section 41) and the Quebec Act respecting Access to Documents Held by Public Bodies and the Protection of Personal Information (R.S.Q., c. A-2 1; see especially Section 61 and Section 68.1). In France Law No. 78-17 of 6 January 1978 "relative à l'informatique, aux fichiers et aux libertés" is applicable for police files.

306 See, e.g., for Germany, e.g., Sections 7 et seq. Federal Criminal Police Office Act of 7 July 1997; for Italy, Article 4 Data Protection Act of 1997; for Norway Section 9 of Act No. 48 of 9 June 1978 Relating to Personal Data Registers requires permission of the King (i.e. a government concession) for the establishment of specific (especially electronic) personal data registers.

307 See, e.g., for Germany, the Law on the Central and the Education Register of 22 July 1976.

308 For the relevant work of international organisations see infra chapter IV.A.2.b, fn. 379.

data can easily be manipulated (a phenomenon which is illustratively described as the "second-hand nature" of computer printouts).[309]

The admissibility of evidence from computer records in courts depends to a great extent on the underlying fundamental principles of evidence in the respective country. Two main groups of countries must be differentiated: continental law countries on one the hand (infra a) and common law countries on the other hand (infra b).

a. Continental Law Countries

The Continental law countries and many others operate according to the principle of free introduction and free evaluation of evidence ("système de l'intime-conviction").[310] In these countries the judge can, in principle, use all kinds of evidence and then has to weigh the extent to which he can rely on the evidence (especially his own observations, the statements of suspects, witnesses and experts, as well as written documents). Legal systems based on these principles in general do not hesitate to introduce computer records as evidence.[311] Problems occur only when procedural provisions provide specific regulations for the proof of judicial acts or proof with legal documents.[312] For example, in France, in the field of civil law, a legal amendment of 1980 on Proof of Judicial Acts introduced new possibilities of proof of judicial acts according to which, under certain conditions, originals can be replaced by reliable copies.[313]

---

309 See *Amory/Poullet*, Computer Evidence – A Comparative Approach in Civil and Common Law Systems, International Computer Law Adviser Volume 1, No. 4, January 1987, pp. 7 et seq., February 1987, pp. 12 et seq.; *Sieber*, The International Handbook on Computer Crime, 1986, pp. 20, 139 et seq. The following chapter is based on chapter IV.C.1 of this book.

310 For Germany see for example Section 261 of the Criminal Procedural Code.

311 Another question is how an electronic evidence is considered by the court. The Federal Court of Justice in Germany for example has decided, that the "o.k."-sign of a fax maschine does not always prove the arrival ((1995) Neue Juristische Wochenschrift, pp. 665 et seq.). Because of the possibilities of manipulation the value of an electronic evidence depends on the general reliability and manipulability of a certain system. In addition to that, computer for example computer printouts (especially by laser printers) are much less individual than former times' typewriters.

312 See, e.g., for the delimitation of "document" and "object of real evidence" ("Urkunde" and "Augenscheinsobjekt") in the criminal procedural law of Germany, Entscheidungen des Bundesgerichtshofs, Volume 14, pp. 339 et seq. and Volume 27, pp. 135 et seq.; for the delimitation of "written material" in the field of information technology in the Netherlands, Dutch Committee on Computer Crime, Information Technology and Criminal Law ("Franken report"), English translation, 1987/88, pp. 90 et seq. (nos. 156, 157); for Greece, Articles 177, 179 Criminal Procedural Code.

313 See for France, Law No. 80-525 of 12 July 1980 on Proof of Judicial Acts; Section 1348 Civil Code; for similar questions of civil procedural law in Germany compare *Bohatiuk*, Beweiswert gespeicherter Informationen, (1986) Computer und Recht, pp. 535 et seq., at 538 et seq.; *Köhler*,

b. Common Law Countries

Contrary to the legal situation in continental law countries, the common law countries, especially Australia, Canada, the United Kingdom and the United States of America, are, to a greater extent, characterised by an oral and adversarial procedure. In these countries a witness can only testify concerning his personal knowledge, permitting his statements to be verified by cross-examination. Knowledge from secondary sources, such as other persons, books, or records, is regarded as "hearsay evidence", and is, in principle, inadmissible. So the qualifications of electronic evidence as hearsay and traditional rules of best evidence do not favour their use. However, in general it can be said that there are several exceptions to the hearsay evidence rule, such as the "business records exception" or the "photographic copies exception" and that moreover the modern judge does not any longer close his eyes for electronic evidence.[314] The business records exception, for example, permits a business record created in the course of everyday commercial activity to be introduced as evidence even if there is no individual who can testify from personal knowledge. Since most of these common law rules were developed in the 19th century and reflect the problems of Victorian society, the question whether computer files are "real evidence" and the question whether or not computer printouts fall under one of this exceptions of the hearsay rule have been the subject of extensive debate.[315] Some common law countries have accepted computer printouts as falling within the business records exception. Others have elaborated new laws allowing computer records to be admitted as evidence if certain conditions are met.

Die Problematik automatischer Rechtsvorgänge, insbesondere von Willenserklärungen, 182 (1982) Archiv für die zivilistische Praxis, pp. 126 et seq.

314 Cf. also the Recommendation of the Council of Europe on Criminal Procedural Law 1995, principle 13: "The common need to collect, preserve and present electronic evidence in ways that best ensure and reflect their integrity and irrefutable authenticity, both for the purposes of domestic prosecution and international co-operation, should be recognised. Therefore, procedures and technical methods for handling electronic evidence should be further developed, and particularly in such way as to ensure their compatibility between states. Criminal procedural law provisions on evidence relating to traditional documents should similarly apply to data stored in a computer system."

315 See, e.g., The Australian Law Reform Commission, Evidence Volume 1, Interim Report No. 26, 1985, pp. 356 et seq.; *Bequai*, How to Prevent Computer Crime, 1983, pp. 97 et seq.; *Brown*, Computer-Produced Evidence in Australia, University of Tasmania Law Review Volume 8 (1984); *Kelman/Sizer*, Computer Generated Output as Admissible Evidence, 1982; *Kyer*, Computer Records as Courtroom Evidence, Volume 1 No. 8 (August 1984) Computer Law, pp. 57 et seq., Volume 1, No. 9-10 (September/October 1984), pp. 76 et seq.; *Reed*, A Note on Criminal Evidence, in: Reed (ed.), Computer Law, 1990, pp. 194 et seq.; *Tapper*, Computer Law, 3rd ed. 1983, pp. 16 et seq.

In the United Kingdom, the Police and Criminal Evidence Act of 1984[316] provides in Section 69 (a) that a statement in a document produced by a computer must satisfy the following conditions in addition to the general requirements for admissibility of documents to be used as evidence: "(1) That there are no reasonable grounds for believing that the statement is inaccurate because of improper use of the computer; (2) That at all material times the computer was operating properly, or, if not, that any respect in which it was not operating properly or was out of operation was not such as to affect the production of the document or the accuracy of its contents; and (3) That any relevant conditions specified in rules of court under Subsection 2 below are satisfied." Part II of Schedule 3 of the Act which supplements Section 69 by making more detailed provisions as to the admissibility of computer evidence, provides in paragraph 11 that in estimating the weight of a statement admissible under Section 69 consideration shall be given to all the circumstances, including contemporaneity and the question whether any person who was in a position to do so had any incentive to conceal or misrepresent the facts. In addition to the accuracy requirements of the Police and Criminal Evidence Act 1984, documents must come under one of the exceptions to the hearsay rule of the Criminal Justice Act 1988 if they are not "real evidence" (such as information collected directly by the computer itself) but "hearsay evidence" (such as records containing observations made by a human being).[317]

Australian law tackles the problem by using two different approaches which can be classified as the "computer-specific" approach and the "business records" approach; in some jurisdictions both concepts are adopted simultaneously. The "computer-specific" approach uses legislative provisions that are specifically aimed at the admissibility of computer-

316 For details of the act see *Zander*, The Police and Criminal Evidence Act 1984, 1985 (Reprint 1988); *Hargreaves/Levenson*, A Practitioner's Guide to the Police and Criminal Evidence Act 1984, 1985. For the admissibility of computer printouts under Sections 68 and 69 of the act compare *R. v. Minors/R. v. Harper*, Decision of the Court of Appeal (Criminal Division), (1985) The Criminal Law Review, pp. 360 et seq.

317 Section 24 of the Criminal Justice Act 1988 (replacing Section 68 of the Police and Criminal Evidence Act 1984) provides that documents arising from trade, business, professional, occupational or official activities which record information supplied by a person who has personal knowledge of the matters recorded are admissible in criminal proceedings under the requirements of Section 23 (2) or Section 24 (4) (iii). Under Section 23 (2) the document is admissible if the person who would otherwise give oral evidence is dead or unfit to testify, if he is abroad and it is not practicable for him to testify, or if he cannot be found although reasonable steps have been taken to find him. Section 24 (4) (iii) permits the document to be given in evidence if the maker of the statement cannot reasonably be expected to remember the matters contained in the record.

produced evidence.[318] The "business records" approach considers computer-produced evidence only as one aspect in the general question of admissibility of business records.[319]

In the United States of America, several state laws contain provisions which specifically address problems of evidence. In 1983 the Evidence Code of California was amended by Section 1500.5 which is identical to Section 3 of the Suggested State Legislation of the State Governments Committee. The section stated that "computer-recorded information or computer programs, or copies of computer-recorded information or computer programs, shall not be rendered inadmissible by the best evidence rule". A printed representation of computer information or computer programs shall be admissible to prove the existence and content of the computer information. The printed representations will be presumed to be accurate representations of the computer information which they purport to present. This presumption, however, only affects the burden of producing evidence since the party which introduces the printed representation will have the burden of proving, by a preponderance of evidence, that it is the best available evidence of the existence and content of the respective computer information or computer programs, when there is proof that the document is inaccurate or unreliable. In Iowa the computer crime law of 1984 in Section 716A.16 simply created a new rule, saying that "in a prosecution under this chapter, computer printouts shall be admitted as evidence of any computer software, program, or data contained in or taken from a computer, notwithstanding an applicable rule of evidence to the contrary".[320]

Similar problems are discussed in Japan, where hearsay evidence generally is excluded as evidence and the exception of business records can be applied in specific cases.[321]

---

318 Such provisions can be found for Australia in the Capital Territory (Part VII of the Evidence Ordinance 1971), in Queensland (Section 95 of the Evidence Act 1977), and in South Australia (Part VI A of the Evidence Act 1929-83).

319 For Australia it is used in the Capital Territory (Section 29 (2) of the Evidence Ordinance 1971), in the Commonwealth (Part III A of the Evidence Act 1905), in New South Wales (Part II C of the Evidence Act 1898), in Queensland (Section 93 of the Evidence Act 1977), in South Australia (Section 45a of the Evidence Act 1929-83), and in Victoria (Section 55 of the Evidence Act 1958).

320 For an overview on the relevant law of the USA see *Bloom/Becker*, The Computer Crime Law Reporter (loose-leaf edited by the National Centre for Computer Crime Data, Los Angeles).

321 See for Japan, Articles 320, 323 Criminal Procedural Code.

5. "Extraterritorial" Application of National Computer Crime Statutes

The international range of criminal law provisions creates problems in international computer networks especially since the middle of the 1990s with respect to illegal and harmful contents on the Internet: Based on the principle of territoriality, many states do not only apply their criminal laws on illegal contents (such as pornography or hate speech) in cases in which these contents are stored on a server in their country. Considering not only the place of commission but also the place of potential results,[322] they also extend their jurisdiction to cases in which servers are set up abroad but can be accessed from their country. Using this doctrine of "(potential) effect of the crime", e.g. the German criminal law system claims jurisdiction on the authors of statements and the operators of servers in Canada which act in accordance with Canadian law but which infringe German anti-nazi legislation if the Canadian servers are accessible from Germany. A consequent application of this doctrine of "(potential) effect of the crime" leads to the result that European service providers are also subject to Islamic law if their contents are accessible e.g. from Iran. Generally speaking, one could say that under this doctrine of law, a service provider on the Internet is subject to nearly all legal orders of the world.[323] A few authors hold *de lege lata* the opinion that national criminal law is only applicable if the perpetrator has acted in the state or intended to produce a result just in a certain state.[324]

The resulting conflicts of law are aggravated by the fact that jurisdiction in criminal matters in many countries it not only determined by the principle of territoriality, but also by other principles such as the principle of universal

322 See, e.g., Sections 3, 9 German Criminal Code; Sections 62, 67 (2) Austrian Criminal Code; Section 9 Danish Criminal Code; Section 10 Finnish Penal Code and Sections 3 (1), 7 (1) Swiss Criminal Code.

323 See for the international applicability of national criminal law with respect to offences on the Internet *Hilgendorf*, Überlegungen zur strafrechtlichen Interpretation des Ubiquitätsprinzips im Zeitalter des Internet, (1997) Neue Juristische Wochenschrift, pp. 1873 et seq. *Riklin*, Information Highway und Strafrecht, in: Hilty (ed.), Information Highway, 1996, pp. 559 et seq., at pp. 579 et seq.; *Ringel*, Rechtsextremistische Propaganda aus dem Ausland im Internet, (1997) Computer und Recht, pp. 302 et seq. For an discussion in the Internet itself see the debate between Post and Goldsmith <http://www.hotwired.com/synapse/braintennis/97/34/index0a.html> (accessed on 21 January 1998). Similar problems appear in international civil law, see for example *Stäheli*, Kollissionsrecht auf dem Information Highway, in: Hilty (ed.), Information Highway, 1996, pp. 597 et seq.

324 Cf. *Piette-Condol/Bertrand*, Internet et la loi, 1997, p. 61; *Widmer/Bähler*, Rechtsfragen beim Electronic Commerce, 1997, pp. 305 et seq.; *Collardin*, Straftaten im Internet, (1995) Computer und Recht, pp. 618 et seq.

prosecution (applicable e.g. with respect to child pornography in many countries).[325]

In all countries until now, there are no solutions how to protect citizens efficiently against illegal contents on the Internet while avoiding intolerable conflicts of law at the same time. Such solutions cannot be found on the national level but only on the international level by creating a universal minimum code of rules which are applicable in all countries.

6. Consequences for International Co-operation

Computer-related crimes have a strong international dimension and so has its investigation: The ubiquity of information in modern communication systems makes it irrelevant as to where perpetrators and victims of crimes are situated in terms of geography. There is no need for the perpetrator or the victim of a crime to move or to meet in person. Illegal actions such as computer manipulations in one country can have direct, immediate effects in the computer systems of another country, thus leading to damages e.g. to life or property or to the dissemination of unlawful material in international computer networks.[326] The Internet shows that frontiers between countries do not factually interfere with the Internet traffic and do not prevent Internet users to exchange information and eventually to enter into electronic agreements. On the contrary, law enforcement authorities generally have to respect the borders of their states. As representatives of the national state they can only act legally within their own jurisdiction, unless international treaties provide a clear legal basis.[327]

Thus, the international character of computer networks calls for international co-operation of police and law-enforcement authorities. The precondition for such an international co-operation is that police and other law enforcement authorities dispose of adequate and similar powers on the basis of national law. Under all agreements on police co-operation and

325 See, e.g., Section 6 No. 6 of the German Criminal Code; cf. also Section 64 (I) No. 4a Austrian Criminal Code.

326 See *Sieber*, The International Handbook on Computer Crime, 1986, pp. 114 et seq.; *Sieber*, The International Emergence of Criminal Law, 1992, pp. 97 et seq. That is also why in the field of substantive criminal law computer crimes are the field where harmonisation is indispensable, because a national control is no longer possible.

327 Cf. the recommendations in the United Nations Manual on the prevention and control of computer-related data, part VI D, UN, international review of criminal policy Nos. 43 and 44, 1994. As a typical example of international co-operation see the Benelux Treaty of 27 June 1962 on Extradition and Mutual Assistance in Criminal Matters.

mutual assistance, states can only provide measures which are admissible under their national law.[328] Thus, there is an international interest that the legal systems of all countries contain not only harmonised provisions in the field of substantive law, but also adequate criminal procedural law provisions, especially in the field of coercive powers.

7. Comparative Analysis

The applicability of computer-related criminal procedural law is not only relevant in the prosecution of substantive computer crime as described above in this report but rather has implications for a wide variety of criminal acts. However, this fundamental importance of computer-related criminal procedural law is at present only partially reflected in the laws of the countries analysed.

With respect to the gathering of information the *scope of coercive powers* of the prosecuting authorities proves particularly problematic: While activities not affecting a third party's constitutional rights (such as "electronic police patrols" in public areas of the Internet) do not pose legal problems, all coercive powers in general require a statutory basis. In particular in countries where an analogous application of criminal procedural law is not possible, this may create significant problems for law-enforcement unless laws are amended to cover the specific needs of computer- and network based investigations.

In the area of *search and seizure*, it still remains an open issue in most countries whether data *per se* can be the subject of search and seizure or whether the relevant statutes only apply to the data carrier itself. The latter may be disproportionate if for example a complete server is seized only to secure one small file. In many countries, it is also unclear who should ultimately bear the costs of such a measure, whether police can use computer equipment of suspects and witnesses and whether the police should be allowed to access connected servers online (especially if they are located outside the premises mentioned in the search warrant or even located abroad).

With respect to *wire-tapping* it is accepted in most countries that the relevant provisions apply not only to voice telephony but to all kinds of communications via telecommunication. It is, however, unclear in most

328 This procedural law requirement must not be mixed up with the substantive law requirements of "double criminality" which exist in addition.

jurisdictions whether these rules can also be used when a mail server is accessed online in order to retrieve data stored there.

Duties imposed on third parties to actively co-operate with law enforcement (for example when data are encrypted or otherwise cannot be read without the help of a third party) are highly relevant in the field of computer-related criminal procedural law. However, only a few states already dispose of such powers in their procedural law. In order to solve the relevant problems, countries should regulate active duties of co-operation as was done in the Netherlands.

The use of *computer-generated evidence* in court has posed legal difficulties in the past only in common law countries. This type of evidence has become widely admissible now. However, in all countries, one has to bear in mind the fact that such data are also highly susceptible to manipulations.

Creating an adequate system of procedural law is not only a national law problem. Since countries in legal assistance matters (even if double criminality is provided) can only provide measures admissible under their national law, there is a strong international interest in creating a clear legal basis for investigations in computer and communication systems all over the world.

F. Regulations on Protection Measures

The computer crime cases described above have not only led to problems of substantive and procedural criminal law. They have also raised the question whether security measures against computer crime should be regulated by administrative law. The discussion of these questions which goes beyond the topic of this report is quite complex and can only be briefly pointed out here. In principle, three different questions must be distinguished: obligations to implement protection measures (infra 1) , prohibitions of certain protection measures (infra 2), and consequences of possible manipulations for the use of electronic contracts (infra 3).

1. Obligations for Security Measures

A *general duty to implement safeguard measures* for the protection of data processing systems does not exist for the private sector (unlike the situation in the public sector). In a free society and market economy, the individual citizens are free to decide whether they want to protect their individual

interests or at least their computer systems by costly measures or whether they are ready to accept the risk of an "electronic burglary".

However, this principle is not valid if the lack of safeguard measures does not only lead to the infringement of interests of the respective computer user, but also infringes the interests of third parties (especially privacy rights) and of public interests (such as the interest in a functioning network). In these cases, the legislator sometimes demands adequate measures for the protection of these persons (who in most cases cannot decide themselves about the implementation of safeguard measures) and for the protection of general interests.

a. Protection of Personal Data

Obligation for security measures exist above all for computer users that process personal data of third parties, e.g., insurance companies, credit inquiry agencies or telecommunications operators. In this respect, reference can be made to the general explanations above concerning the field of data protection law.[329] E.g., in Germany, Section 9 of the general Data Protection Law requires technical and organisational security measures which are specified in an annex to that law. Moreover, there are specific provisions in sectorial regulations, e.g., for the protection of telecommunication secrecy (Section 87 (1) Telecommunications Act[330] and Section 4 (2) No. 3 Teleservices Data Protection Act) and for the secrecy of telecommunications supervision (Section 12 Telecommunications Supervision Ordinance).[331] Corresponding regulations can be found in the new Telecommunications Services Companies Data Protection Ordinance.[332]

The development in other countries is similar as far as the general provisions of data protection law are concerned,[333] whereas regulations in sectorial laws are not so widespread, e.g. in Finland, Section 26 of the Personal Data File Act regulates the duty to implement adequate security measures.[334] In Spain, Articles 9 and 31 of the Law 5/1992 for the Regulation of the Automated Processing of Personal Data (LORTAD) provide that the persons responsible for the data processing must take the necessary safety

329 Cf. above II.A.

330 Bundesgesetzblatt I, 1996, pp. 1117 et seq.

331 Bundesgesetzblatt I, 1995, p. 722.

332 Bundesgesetzblatt I, 1996, pp. 961 et seq.

333 Cf. the summary of *Sieber*, in: Cheswick/Bellovin (eds.), Firewalls und Sicherheit im Internet, 1996, pp. 309 et seq.

334 Cf. the Finnish report in the Annex, page 180.

measures in order to protect personal data against unauthorised access, changes etc.[335] Moreover, regulations with regard to the protection of data of third parties can be found in Canada, e.g., Section 244 Bank Act, Section 240 Cooperative Credit Associations Act, Section 10 Act concerning Canadian Business Corporations, Section 266 Insurance Companies Act and Section 248 Trust and Loan Companies Act.[336]

b. Protection of Public Interests

Duties to implement security measures can also exist to protect special public interests. This includes e.g. the protection of telecommunications facilities against damage. Another example is the call for safe technical components when creating signature keys which are necessary for the use of digital signatures,[337] in order to prevent, e.g., that a private signature key is used by an unauthorised person.

In Germany, there are corresponding special legal rules, e.g., for the protection of the public telecommunications network against damages by "terminal equipment" (Section 59 Telecommunications Act). In the field of digital signatures, Section 5 (4) and (5), Sections 10 and 14 German Digital Signature Act regulate the security requirements to be observed by the certification authorities, mainly in order to ensure the integrity of the signature keys and the corresponding personal data.[338] These requirements are specified in further detail by the Digital Signature Ordinance enacted on the basis of Section 16 Digital Signature Act. The Ordinance provides for corresponding rules in Sections 10, 11, 12, 13, 15, 16 and 17.[339] The legal situation in the other countries that are the subject of this study has not been examined yet.[340]

---

335 Cf. the Spanish report in the Annex, page 541.

336 Cf. chapter 2, pp. 6 et seq. of the study of the Canadian Ministry of Justice "A Survey of Legal Issues Relating to the Security of Electronic Information", to be found at <http://canada.justice.gc.ca/Commerce/index_en.html> (accessed on 21 January 1998).

337 For digital signatures, see supra III.F.3.

338 Bundesgesetzblatt I, 1997, pp. 1869, 1873 et seq.

339 The Digital Signature Ordinance can be obtained at <http://www.iid.de/rahmen/sigv.html> (accessed on 21 January 1997); also cf. the legislative intent of the German Federal Government concerning this Ordinance at <http://www.iid.de/rahmen/sigv_begr.html> (accessed on 21 January 1998).

340 As far as we know, regulations in special laws that deal with security measures in the public interest do not exist in the other Member States of the EU.

2. Prohibitions of Security Measures

Similarily, *prohibitions of security measures* can exist mainly for two reasons: Such prohibitions can protect third party interests (such as privacy rights). They can also protect public interests (such as the interests of prosecuting agencies to supervise encrypted data).

a. Protection of Privacy

Prohibitions of security measures with respect to privacy rights can be applicable if personal activities of internal or external users of a computer system are recorded for safety reasons. The scope of relevant cases ranges from the recording of attempts to get unauthorised access to a computer, via the recording of connection data at the router, to the content supervision of discussion forums and electronic mail. It is obvious that such recordings can infringe privacy rights of the supervised or controlled persons.

In Germany, the respective supervision measures are not covered by the provisions of the Criminal Code, but only by general and specific data protection laws. Specific German regulations can mainly be found in Section 89 (4) Telecommunications Act[341] and in Sections 3 et seq. Telecommunications Services Companies Data Protection Ordinance.[342] In the field of the use of teleservices, Sections 3, 4, 5 and 6 Teleservices Data Protection Act regulate the admissibility of the collecting and processing of personal data.[343] Comparative studies as well as an international co-ordination are still lacking in this field.

b. Prohibitions of Cryptography

General prohibitions of security measures for the protection of public interests are discussed in particular in the field of cryptography in order to allow law enforcement authorities and secret services to listen in on data communication. In spite of this discussion, legal provisions prohibiting the use of cryptography exist only on a very limited scale in the Member States of the EC.

The most restrictive provisions in this respect can be found in France. The use of cryptography, in particular for the protection of secrecy, used to

341 Bundesgesetzblatt I, 1996, pp. 1117 et seq.

342 Bundesgesetzblatt I, 1996, pp. 961 et seq.

343 Bundesgesetzblatt I, 1997, pp. 1869, 1871/1872

be practically forbidden by the Law No. 90-1170[344] of 29 December 1990 (together with the Decree No. 92-1358 of 28 December 1992). The situation is now somewhat less restrictive because of Article 28 of the Law No. 96-659 of 26 July 1996 (French Telecommunications Act),[345] which has still got to be implemented by a decree. According to this provision, the use of cryptography software and/or hardware is permitted if it is exclusively used for the authentication or securing of the integrity of information. This concerns mainly the use of digital signatures. However, if the encryption technology is also used for the safeguarding of secrecy, the secret key used must be deposited at a "trusted third party" ("TTP"). This trusted third party has to hand out the secret key to the public authorities under certain circumstances described in further detail in the French Telecommunications Act. The French legislator thus in principle requires – unlike all other Member States – the creation of a "key escrow system" for the use of cryptography for the protection of secrecy. The Telecommunications Act further provides that TTPs need a public authorisation and must be established in France. Irrespective of the deposit of a secret key with a "trusted third party", the French Prime Minister can grant permission for the use of cryptography. A Working Group of the French Ministry for Finance and Economy demands, however, in its final report on the development of electronic commerce published at the beginning of 1998, that future rules in the field of cryptography must be marked by a "liberal spirit", so that the existing opportunities in the field of electronic commerce can be effectively used.[346]

In Austria, Section 20 of the Business Radio Communication Ordinance ("Betriebsfunkverordnung") prohibits the use of cryptography in radio networks, unless the communication is effectuated among organisational entities of the Federal Ministry of the Interior.[347]

In the United Kingdom, the creation of a TTP infrastructure comparable to the system envisaged in France was discussed.[348] Specific laws, however, do not yet exist, which is in particular due to the change of the British Government. The new Labour Government has pointed out in an official

344 Cf. <http://www.dmi.ens.fr/equipes/grecc/Crypto/loi.html> (accessed on 21 January 1998).

345 Cf. <http://www.telecom.gouv.fr/english/activ/telecom/nloi17.htm> (accessed on 21 January 1998).

346 Cf. <http://www.finances.gouv.fr/commerce_electronique/lorentz/anglaise/rapporte.htm> (accessed on 9 January 1998).

347 Austrian Bundesgesetzblatt No. 639/1995.

348 Cf. <http://dtiinfo1.dti.gov.uk/pubs/> (accessed on 21 January 1998).

statement that it does not envisage the creation of a key escrow systems.[349] Similarily, in Germany, plans of the Ministry for Interior Affairs for regulations of cryptography could not win through against the more liberal positions of the Ministry for Economic Affairs.

The situation in the US is a lot more complex, even though there are no laws restricting the domestic use of cryptography either. In the US, the discussion already began in 1993 with the so-called "Clipper-Initiative". At that time, the Clinton Administration introduced the "Escrowed Encryption Standard" (EES), which enabled public authorities to directly decode encoded communication.[350] The EES was first implemented on the Clipper Chip, which was to be used, e.g., in cellular phones. Even though the EES could not succeed due to considerable concerns in view of the protection of privacy, the US Government at first pursued the creation of a "key escrow system" (so-called Clipper II-, Clipper III- and Clipper IV-initiatives), in which the public authorities should be in possession of the keys necessary for decoding. Only at the beginning of 1997, the Clinton Administration turned towards a "key recovery system", i.e. towards the creation of a "public key infrastructure (PKI)". According to this concept, the required information shall be deposited at so-called "key recovery agencies (KRA)", so that the decoding of encoded information or communication is possible. This information shall be issued to public authorities under certain circumstances specified by law. Moreover, registered certification authorities (CAs) – which are in charge of the certification of public keys – shall only certify a public key, if the holder of this key has revealed sufficient information to the KRA.[351] Similar legislative proposals have been worked out in Congress and are named after one or more senators respectively.[352] Because of a lengthy American legislative procedure and the intense public discussion in the USA, a definite legal regulation is probably not to be expected soon.

c. Export Controls on Cryptography

The situation in the field of the export of cryptography is somewhat different. In Belgium, a licence is required if cryptography is to be exported

349 Cf. <http://www.labour.org.uk/views/info-highway/content.html> (accessed on 21 January 1998).

350 A survey can be found at <http://www.epic.org/crypto/clipper/fips_185_clipper_feb_94.html> (accessed on 5 January 1998).

351 Cf. <http://www.cdt.org/crypto/970312_admin.html> (accessed on 22 January 1998).

352 See for the respective draft bills <http://www.cdt.org/crypto/legis_105/pro_CODE/> (accessed on 21 January 1998).

to countries outside the Benelux-countries.[353] In France, the export is regulated by the above-mentioned Law No. 90-1170 of 29 December 1990[354] and in Sweden by the Laws SFS 1994:2060 and SFS 1995:1680.[355] Additionally, the export of cryptography technology in all Member States of the EU is regulated by the 1994 Council Regulation on dual-use goods[356] and supplemented by various national laws.[357]

In Canada, export restrictions for cryptography are determined by the "Export and Import Permits Act".[358] In the US, the piece of legislation applicable to the export of cryptography up to the end of 1996 was the "International Traffic in Arms Regulation (ITAR)", because cryptography was on the "United States Munition List". The State Department was in charge of granting export licences.[359] On the basis of the Clinton Administration's "Executive Order on Export Controls" of 15 November 1996,[360] the Department of Commerce is now in charge of the licensing, in which other Government Departments such as the Department of Justice must participate. Cryptography now figures in the "Commerce Control List" and is thus subject to the "Export Administration Regulations" of 30 December 1996.[361] According to these rules, a six-months export licence is granted after a single control for cryptography that uses at most a 56-bit key, if the manufacturer agrees to implement a key recovery system within two years. This time period begins on 1 January 1997 and ends on 31 December 1998. If no key recovery system is implemented by this date, the old rule is valid again, i.e. only the export of cryptography with a maximum key length of 40 bit is permitted. According to a statement of the Clinton Administration of 1 October 1996, a stronger cryptography than a 56-bit key will be allowed if a key recovery system is immediately provided

353 Cf. <http://www.cwis.kub.nl/~frw/people/koops/cls2.htm> (accessed on 22 January 1998).

354 Cf. supra fn. 344.

355 See <http://www.notisum.se/rnp/sls/lag/19942060.htm> (accessed on 21 January 1998) and <http://www.notisum.se/rnp/sls/lag/19951680.htm> (accessed on 21 January 1998).

356 Council Regulation (EC) No. 3381/94 of 19 December 1994 on setting up a Community regime for the control of export of dual-use goods, OJ L 367/1 of 31.12.1994; amended by Council Regulation (EC) No. 837/95 of 10 April 1995, OJ L 90/1 of 21.04.1995.

357 Cf., e.g., for Germany Außenwirtschaftsgesetz, Bundesgesetzblatt I, 1961, pp. 481 et seq. and Außenwirtschaftsverordnung, Bundesgesetzblatt 1993, pp. 1937 et seq.

358 Cf. *Piragoff*, Canadian report, p. 59.

359 Cf. <http://www.cwis.kub.nl/~frw/people/koops/cls2.htm> (accessed on 22 January 1998).

360 Cf. <http://www.epic.org/crypto/export_controls/executive_order_11_15_96.html> (accessed on 21 January 1998).

361 Cf. <http://www.eff.org/pub/Privacy/ITAR_export/961230_commerce.regs> (accessed on 21 January 1998).

by the manufacturer.[362] Because of this legal situation which is dissatisfying especially for the manufacturers of software and hardware that use encryption technology, there are some proposals that intend to facilitate the export of cryptography. Among the proposals to be mentioned are the draft "Security and Freedom through Encryption Act" (SAFE) and the draft "Promotion of Commerce Online in the Digital Era Act" (Pro-CODE).[363] Both draft bills aim to facilitate the export of generally accessible and public-domain cryptography software. Moreover, the Federal District Court of San Francisco has decided in the "Bernstein Case" that export restrictions for cryptography in this particular case violate the First Amendment and are thus anti-constitutional.[364]

3. Digital Signatures

The manipulation possibilities described above lead to the additional question as to what extent *contracts* concluded via data networks should be recognised. In practice, the use of digital, encoded signatures tries to safeguard that a document originates from a certain person (authentication) and that it cannot be falsified.

In Germany, the Digital Signatures Act is in force since 1 August 1997.[365] The legislator has knowingly refrained from regulating whether digital signatures are legally binding and only deals with the necessary infrastructure for the use of digital signatures such as the tasks of the certification entities. Further detailed legal rules are provided by the Digital Signature Ordinance of 8 October 1997 enacted on the basis of Section 16 Digital Signatures Act. In the other EU Member States, there are no laws dealing with the use of digital signatures. Initiatives or draft bills can be found in Denmark,[366] the UK,[367] Italy[368], and Sweden[369] as well as in Japan.[370]

362 Cf. <http://www.eff.org/pub/Privacy/ITAR_export/961001_wh_clipper3.statement> (accessed on 21 January 1998).

363 Cf. <http://www.cdt.org/crypto/legis_105/SAFE> (accessed on 21 January 1998) and <http://www.cdt.org/crypto/legis_105/pro_CODE> (accessed on 21 January 1998).

364 However, this decision only means that the mathematician *Bernstein* can export the source code of his cryptography software. Cf. <http://www.cdt.org/crypto/bernstein.shtml> (accessed on 21 January 1998).

365 See Article 3 Information and Communication Services Act.

366 Cf. <http://www.fsk.dk/fsk/publ/elcom/kap02.htm> (accessed on 21 January 1998).

367 Cf. <http://dtiinfo1.dti.gov.uk/pubs> (accessed on 21 January 1998).

368 Cf. <http://www.aipa.it/notaria/atti_ele.htm> (accessed on 21 January 1998).

In the US the situation is different: In most federal states, there are laws that frequently not only regulate the infrastructure, but also deal with the legal effects of digital signatures.[371] Moreover, on the federal level, there is the "Digital Signature Standard (DSS)", which provides a means of authenticating the integrity of electronically transmitted data and the identity of the sender. The standard is applicable to all federal departments and agencies for the protection of unclassified information.[372]

4. Comparative Analysis

Obligations to implement security measures in the private interest mainly result from general data protection laws in so far as the protection of personal data is concerned. Special legal rules in this regard are quite rare and concern various fields such as telecommunications in Germany or the banking and insurance sector in Canada. Further regulations with respect to security measures exist in the field of the reliable creation of cryptographic keys. In this field there is a particular need for national legislators to catch up.

As far as the *prohibition of security measures* is concerned, general data protection laws as well as some specific sectorial privacy laws prohibit a too excessive collection of personal data. However, in this field (which lies outside the scope of the present study and ist underlying contract), legal comparative analysis has not yet really started. Furthermore, the prohibition of cryptography is controversially discussed. Even among the Member States of the EU, there are different approaches: Whereas France completely prohibits, respectively limits, the use of cryptography, it can be used without restrictions, e.g., in Germany and also within the US. Some countries such as the US and also Belgium, France or Sweden, regulate the export of encryption technology.

The use of cryptography is also needed for the creation of digital signatures, which allow safe commerce via open data networks. However, in most countries there are no legal provisions for this problem. This situation is especially dissatisfying because a more rapid growth of electronic commerce and thus the creation of new jobs in the service sector is

369 Cf. <http://www.dsv.su.se/~jpalme/SOU-1996-40-eng.html#RTFToC11> (accessed on 21 January 1998).

370 Cf. <http://www.ecom.or.jp/eng/output/ca/eng-guideline.htm> (accessed on 21 January 1998).

371 Cf. <http://www.mbc.com/ds_sum.html> (accessed on 21 January 1998).

372 Cf. <http://www.epic.org/crypto/dss> (accessed on 21 January 1998).

hindered. However, it would not be useful if individual countries adopted national rules that are not co-ordinated: If e.g. in the field of digital signatures, a public key is certified only by a national public authority, this certificate cannot enjoy an adequate level of trust without respective agreements among the individual countries.

G. Conclusions

The multitude of new legal problems of computer crime could be traced back to six areas of computer-specific law problems and law reform: Protection of privacy, economic criminal law, protection of intellectual property, protection against illegal and harmful contents, criminal procedural law as well as legal regulations on protection measures.

The above analysis showed that the international harmonisation in this area has reached different levels. These different levels of international harmonisation are not only a result of historical coincidence and cannot only be traced back to the age of the respective problems (which can, e.g., explain the missing development and harmonisation of the new question of law on security measures). An important reason for the differing levels of harmonisation is also due to the fact that – contrary to civil and administrative law – criminal law is still considered as a core matter of state sovereignty and therefore proved to be more resistant to international harmonisation. This latter reason for the different levels of harmonisation in the field of computer crime legislation becomes obvious if the legal analysis differentiates between the relevant prohibitions and the respective sanctions (which are the two basic elements in criminal law provisions) with respect to computer crime:[373]

– In some of the above analysed areas of computer crime legislation, the prohibitions are laid down in independent (civil or administrative) norms to which the criminal statute refers to. This is the case in the field of privacy protection (where the legality of processing personal data is regulated in administrative and civil laws) and the field of copyright law (where the protected works and the illegal acts are defined in civil

373 The provision element of a criminal law statute is primarily addressed to the citizen and lays down the prohibited acts (such as killing a person or igniting a building). The sanction part of criminal statute is primarily addressed to the judge and indicates how infringements against the provision shall be sanctioned. See for this basic distinction between "Verbotsnorm" and "Sanktionsnorm" infra VI.A.1.b.

copyright laws): In both areas the criminal law statutes are based on and refer to these administrative and civil provisions. Since these administrative and civil law provisions are already harmonised to a considerable degree, the scope of the criminal provisions referring to this accessory non-criminal provisions are also harmonised to a certain degree.[374]

- In other areas the prohibitions are created by criminal law statutes themselves (as is the case in traditional criminal law). This is the case in the field of economic criminal law as well as with respect to illegal and harmful contents in computer networks. Since in these areas the relevant prohibitions are generally not harmonised in administrative or civil laws, but in the criminal statutes themselves, they show considerable differences. In the field of computer-related economic crime, these differences have already been balanced to a considerable degree by the early intervention of international organisations; however, there are still considerable differences with respect to the criminalisation of hacking, trade secret protection as well as computer viruses. In the field of illegal and harmful contents, harmonisation of law has not yet really started. The same is true with respect to procedural law which is a core matter of criminal law and in which many computer-related problems have not been adequately dealt with in most national legal orders.

With respect to the functioning of the internal market it is of no matter whether different prohibitions in national laws are created by civil, administrative or criminal law. In practical business it does not make any difference whether international data flows are hindered by administrative provisions (e.g. on privacy protection) or by criminal statutes (e.g. on pornography or illegal gambling). For that reason a harmonisation of the prohibitions in the fields of economic crime as well as with respect to illegal and harmful contents will also be necessary. If this harmonisation should not be possible in the field of criminal law due to on-going resistance of the national states against the harmonisation of criminal law, one has to consider to only harmonise the underlying prohibitions (especially with respect to economic criminal law as well as illegal and harmful contents) and leave it up the Member States how to sanction infringements of these prohibitions. This idea of differentiating between prohibitions and sanctions will be taken up in the final part of this report dealing with the relevant competences of the European Union.

374 Even if the criminalised acts differ in their scope (such as in the field of privacy protection) there are no considerable discrepancies since the differences in criminal law are compensated by the similar prohibitions of administrative and civil law.

In the field of criminal procedural law in most countries adequate legal answers to the new challenges of computer-based investigations are still missing. Some exeptions from this negative result can be found especially in Canada, the Netherlands and the United Kingdom.

IV. International and Supranational Activities

Various international and supranational organisations realised the above described mobility of data, the transnational character of computer crime, and the resulting need for international harmonisation of the respective laws at an early stage. With respect to the international harmonisation of law, the international organisations started various actions which have already considerably influenced and co-ordinated the legal development of national laws. Today, these international actions concern all of the legal areas dealt with above: computer-related infringements of privacy (infra A), computer-related economic crime (infra B), intellectual property protection (infra C), illegal and harmful contents (infra D), computer-related procedural law (infra E), as well as legal regulations on security measures (infra F).

A. Protection of Privacy

1. Harmonisation of Underlying Administrative and Civil Law

In the field of administrative and civil privacy legislation, various international organisations have developed a common approach to privacy protection at an early stage in order to prevent different concepts and national regulations that would impede the transborder flow of data. The major work in this field has so far been accomplished by the OECD, the Council of Europe, and the European Union; further initiatives were conducted by the United Nations, the G7 and the WTO.

a. Organisation for Economic Co-operation and Development

In 1977, the Organisation for Economic Co-operation and Development (OECD) began to elaborate guidelines governing the protection of privacy and the transborder flow of personal data. These guidelines were adopted by the Council of the OECD in 1980 as a recommendation to the Member States. They are not legally binding for the Members but recommend the

implementation of the general principles set forward in the text. The scope of the guidelines covers only natural persons, applies to both the private and public sectors, and includes automated and non-automated data processing. The eight main points of the guidelines concern the principles of collection-limitation, data quality, purpose-specification, use-limitation, security-safeguards, openness, individual participation and accountability. As far as the international application of privacy laws is concerned, the guidelines in principle request free transborder flow of personal data. However, some interests warrant a restriction of such flow, especially if data is re-exported to circumvent the domestic privacy legislation. In the meantime, all 29 Member States[375] of the OECD have endorsed the guidelines.[376]

b. Council of Europe

A more binding international agreement was achieved by the Council of Europe, which has special responsibilities concerning human rights. The *European Convention of Human Rights and Fundamental Freedoms* of 1950 already gives protection to the privacy of individuals in Article 8 (postulating that individuals must be protected from arbitrary interference with their private and family lives) and Article 10 (securing the right of access to information). As a consequence, the Council of Europe addressed the questions of data protection mainly as a question of protection of human rights and privacy whereas in the discussion of the OECD, the question of free flow of information was dominating.

In 1981 the Committee of Ministers of the Council of Europe, which had already addressed privacy concerns since 1968, adopted the *"Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data"*. So far, 17 Member States[377] have ratified this Convention came into effect on 1 October 1985. In contrast to the OECD guidelines, which are voluntary in nature, the Council of Europe Convention is a

375 Australia, Austria, Belgium, Canada, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, South Korea, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, Spain, Sweden, Switzerland, Czech Republic, Turkey, United Kingdom, the United States of America.

376 For the OECD Guidelines see OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1980; OECD, Transborder Data Flows and the Protection of Privacy, 1979; OECD, Transborder Data Flows: An Overview of Issues, Report DSTI/ICCP/83.29 of 11 October 1983. For current information see <http://www.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM> (accessed on 22 January 1998).

377 Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, the Netherlands, Norway, Portugal, Sweden, Slovenia, Spain, United Kingdom.

contractual commitment of the signatory states and is legally binding. The scope of the Convention is limited to natural persons and to automated files. It applies to automated files both in the private and in the public sector. The Convention expresses ten basic principles representing minimal standards which must be incorporated in the legislation of the contracting states. Though similar, these principles are narrower and more specific than those of the OECD. They demand social justification, collection-limitation, information-quality, purpose-specification, limitation of disclosure, security-safeguards, openness, time limitation, accountability, and participation by individuals. Based on the principle of equivalent protection, the main rule of the convention covering transborder data flows between contracting parties is that data flow to a country providing equivalent protection cannot be hindered. However, there are also exceptions to this rule.[378]

Further initiatives of the Council of Europe were undertaken by the Council of Europe's *Committee of Experts on Data Protection*. Since the opening to signature of the Convention, the Committee has pursued a sectorial approach to data protection issues aimed at elaborating guidelines, in the form of non-binding recommendations addressed to the governments of the Member States, for specific data processing facts. The recommendations adopted by the Committee of Ministers concern automated medical databases, personal data used for purposes of scientific research and statistics, personal data used for purposes of direct marketing, personal data used for social security purposes, personal data in the police sector, personal data used for employment purposes and personal data in the area of telecommunication services.[379] A special working party of the

---

378 For the Convention of the Council of Europe see: Council of Europe, Protection of the Privacy of Individuals vis-à-vis Electronic Databases in the Private Sector, Resolution No. (73) 22, adopted by the Committee of Ministers of the Council of Europe on 26 September 1973 (1974) and Resolution No. (74) 29, adopted by the Committee of Ministers of the Council of Europe on 20 September 1974 (1975); Council of Europe, Explanatory Report on the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Convention opened for signature on 28 January 1981 (1981); Council of Europe/Committee of Ministers, Recommendation No. R (80) 13 of the Committee of Ministers to Member States on Exchange of Legal Information Relating to Data Protection (adopted by the Committee of Ministers on 18 September 1980). *Csonka*, Council of Europe Activities Related to Information Technology, Data Protection and Computer Crime, 5 (1996) Information & Communications Technology Law, pp. 177 et seq.

379 See Recommendation No. R (81) 1 on Regulations for Automated Medical DataBases of 23 January 1981; Recommendation No. R (83) 3 on the Protection of Users of Computerised Legal Information Services of 22 February 1983; Recommendation No. R (83) 10 on the Protection of Personal Data Used for Scientific Research and Statistics of 23 September 1983; Recommendation No. R (85) 20 on the Protection of Personal Data Used for the Purposes of Direct Marketing of 25 October 1985; Recommendation No. R (86) 1 on the Protection of Personal Data Used for

Committee examined the data protection problems posed by certain aspects of the banking sector, in particular by smart cards and point-of-sale transfers.[380]

In addition, the Consultative Committee, provided by Article 18 of the Data Protection Convention, suggested clauses for inclusion in a model contract designed to ensure equivalent data protection in the context of transborder data flows in 1990.[381]

c. European Union

Likewise, the European Community started to harmonise privacy laws in 1976. In its Resolutions of 8 April 1976 (relating to the protection of the individual against the technical evolution of informatics),[382] of 8 May 1979 (on the protection of the rights of the individual in the face of technical developments in data processing),[383] and of 9 March 1982 (on the protection of the rights of the individual in the face of technical developments in data processing),[384] the European Parliament urged the EC Commission to prepare a Community action and recommended that the Member States should sign and ratify the Council of Europe Convention.[385] This was accomplished by the Commission on 29 July 1981 by issuing a *Recommendation to the Member States* to sign the Council of Europe Convention. In addition, since November 1985, the privacy protection of natural and legal persons was discussed by the "Legal Advisory Board" (formally: the "Legal Observatory") of the EC Commission.[386]

Social Security Purposes of 23 January 1986; Recommendation No. R (87) 15 on the Use of Personal Data in the Police Sector of 17 September 1987; Recommendation No. R (89) 2 on the Protection of Personal Data Used for Employment Purposes of 18 January 1989; Recommendation No. R (95) 4 on the Protection of Personal Data in the area of Telecommunication Services, with particular reference to Telephone Services of 7 February 1995.

380 See Council of Europe, Data Protection in the Banking Sector, Working Party No. R (10), Report of the 1st meeting, Doc. No. CJ-PD-GT 10 (87) 3 of 1 July 1987.

381 See Council of Europe, Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data of 28 January 1981, Doc. No. T-PD (90) 24 of 18 May 1990.

382 OJ C 100/27 of 03.05.1976.

383 OJ C 140/17 of 05.06.1979.

384 OJ C 87/33 of 05.04.1982.

385 OJ C 100/79 of 08.05.1979.

386 See Working Paper "Orientation Proposals for a Community Approach on Personal Data Protection", Doc. LAB of 1 October 1986. A critical analysis of the role of the European Communities in the field of data protection is given by *Einwag*, Grenzüberschreitender Datenverkehr aus der Sicht des Bundesbeauftragten für den Datenschutz, (1990) Recht der

A decisive break-through for the European privacy protection came in September 1990 when the Commission submitted a *draft package with six proposals* in the field of personal data protection and information security:

- a general data protection directive applicable to all personal data files coming within the scope of Community law;
- a resolution extending protection to personal data files not coming within the scope of the Community law;
- a declaration asking for the application of the data protection principles to the personal data held by Community institutions and bodies;
- a recommendation in favour of negotiations for the Community's adhesion to the relevant Council of Europe Convention No. 108;
- a sectorial data protection directive covering the specific requirements of the ISDN and public digital mobile networks sector; and
- a decision in the field of information systems security.[387]

In 1995, the Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data was adopted by the Council and the European Parliament.[388] The Member States of the European Union have to implement the Directive within three years so that the deadline for the implementation ends in October 1998.[389] The EC Data Protection Directive covers the following areas:

- lawfulness of the processing of personal data
- principles relating to data quality
- principles relating to the grounds for processing data
- special categories of processing
- information to be given to the data subject
- the data subject's right of access to data

Datenverarbeitung, pp. 1 et seq.; *Simitis*, Datenschutz und Europäische Gemeinschaft, (1980) Recht der Datenverarbeitung, pp. 3 et seq.

387 See Commission of the European Communities, COM(90) 314 final – SYN 287 and 288 of 13 September 1990.

388 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, OJ L 281/31 of 23.11.1995.

389 For the necessary steps in this process and the current implementation status in the Member States see the first annual report of the Working Party on the Protection of Individuals with regard to the Processing of Personal Data (XV/5025/9-final DE).

- exceptions and restrictions
- the data subject's right to object
- confidentiality and security of processing
- notification
- judicial remedies, liability and penalties
- transfer of personal data to third countries
- codes of conduct
- supervisory authority
- rule-making powers of the Commission

With respect to data protection in the area of telecommunications, the Directive will be supplemented by the ISDN Data Protection Directive. The Council has adopted a common position on this Directive on 12 September 1996;[390] most recently, the European Parliament and the Council agreed on the final version of the Directive after a long conciliation procedure.[391] The implementation date is October 1998, in line with the general Data Protection Directive.[392] The Directive covers the following areas:

- security of services and of networks
- confidentiality of communications
- traffic and billing data
- the right to receive non-itemised bills
- presentation and restriction of caller and connected line identification
- automatic call forwarding
- data contained in directories of subscribers
- unsolicited calls for the purposes of direct marketing.

Furthermore, the Treaty of Amsterdam will incorporate a new Article 213b (respectively Article 286 according to the new numbering introduced by the Amsterdam Treaty) into the EC Treaty. According to the new Article, from 1 January 1999 onwards, Community acts on the protection of individuals

390 Common position (EC) No. 57/96 adopted by the Council on 12 September 1996 with a view to adopting Directive 96/.../EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the telecommunications sector, in particular in the integrated services digital network (ISDN) and in the public digital mobile networks (OJ C 315/30 of 24.10.1996). The Common position is also available on the Internet: <http://www2.echo.lu/legal/en/dataprot/isdn/isdn.html> (accessed on 24 January 1998).

391 The Telecommunications Data Protection Directive was adopted on 1 December 1997 and is not yet published in the Official Journal.

392 The Directive will have to be transposed into national law by 24 October 1998, except for certain aspects of confidentiality of communications for which an additional period until 24 October 2000 has been granted.

with regard to the processing of personal data and the free movement of such data shall apply to the institutions and bodies set up by, or on the basis of, the EC Treaty. Before that date, the Council, acting in accordance with the procedure referred to in Article 189b, shall establish an independent supervisory body responsible for monitoring the application of such Community acts to Community institutions and bodies and shall adopt any other relevant provisions as appropriate.

d. United Nations

In 1989, the General Assembly of the United Nations (UN) adopted the "Guidelines on the Use of Computerised Personal Data Flow".[393] On 14 December 1990, the General Assembly adopted the "Guidelines for the Regulation of Computerised Personal Data Files" in their revised version.[394] The Guidelines contain similar principles as the OECD Guidelines and the Council of Europe Convention. They are non-binding recommendations to the Member States and contain principles with respect to accuracy, purpose specification, access rights, non-discrimination as well as security.[395] Additional efforts for privacy protection were made by the Commission on Human Rights of the Economic and Social Council of the UN.

e. G7 Countries

The G7 Countries[396] addressed questions of privacy protection in 1995 in a conference on the information society. The summary of the chairman recommended to respect privacy rights and to protect personal data.[397]

f. World Trade Organisation

The World Trade Organisation (WTO) has also discussed privacy issues with respect to the free flow of data. Especially in the GATS agreement, it

393 See UN, Guidelines on the Use of Computerised Personal Data Flow, Resolution 44/132, adopted in December 1989, approved on 4 December 1990, UN Doc. E/CN.4/Sub.2/1988/22.

394 UN General Assembly Official Records 45th Session 1990, Supplement No. 49 (A/45/95).

395 See UN Doc. E/CN.4/Sub.2/1988/22, p. 10 Annex I; UN Doc. E/CN.4/1990/72 of 20 February 1990.

396 Canada, France, Italy, Japan, Germany, the UK, the United States of America.

397 Cf. final remarks of the G7 headmeeting "Konferenz über die Informationsgesellschaft" on 26 February 1995, Doc/95/2; *Brühann*, EU-Datenschutzrichtlinie – Umsetzung in einem vernetzten Europa, (1996) Recht der Datenverarbeitung, p. 12 (13).

accepted privacy issues as a justification for limiting international data flows.[398]

2. Harmonisation of Criminal Law

Contrary to the progress achieved in the field of administrative and civil privacy law, international harmonisation in the domain of criminal privacy law has not really progressed yet. Only first approaches to deal with these questions have been undertaken by the Council of Europe, the United Nations and the Association International de Droit Pénal.

a. Council of Europe

The main steps in the field of criminal privacy law have been taken by the Council of Europe. The above-mentioned *Data Protection Convention* of the Council of Europe of 1981 contains, in its Article 10, a provision stating that "each party undertakes to establish appropriate sanctions and remedies for violation of ... the basic principles for data protection." However, this clause leaves it up to the Member States to determine the nature of these sanctions and remedies (civil, administrative or criminal), as well as their scope of application.

Further studies on the harmonisation of criminal privacy law were undertaken in the course of the *Select Committee of Experts for Computer-Related Crime* of the Council of Europe. In his comparative report one of the Committee's Scientific Experts suggested already in 1986 that the harmonisation of law should be extended to the field of criminal law provisions by a two step working plan in order to arrive at an international consensus in this field: First, an appropriate international organisation should aim towards developing certain basic principles which would then be considered by all national legislations in the field of computer-related criminal privacy legislation and which could be presented in the form of a recommendation or convention. Based on these principles, a list of acts of criminal privacy infringements should then be developed. This list of acts could supplement the OECD list mentioned above, should prevent both under- and over-criminalisation, and could be put down in the form of a model law.[399] Following these suggestions, the Committee recommended

398 See *Brühann*, EU-Datenschutzrichtlinie – Umsetzung in einem vernetzten Europa, (1996) Recht der Datenverarbeitung, p. 12 (18).

399 See *Sieber*, Proposal for a Council of Europe Initiative in the Field of Computer-Related Infringements of Privacy, Council of Europe Doc. No. PC-R-CC (86) 11 of 26 March 1986, and

basic principles which should be taken into account by all Member States when acting in the field of computer-related criminal privacy legislation. These basic principles were the following:

"(1) The protection of privacy against offences caused by modern computer technology is of great importance. However, this protection should be based primarily on administrative and civil law regulations. Recourse to criminal law should be made only as a last resort. This means that criminal sanctions should be used only in cases of severe offences in which adequate regulation cannot be achieved by administrative or civil law measures (Ultima ratio principle).

(2) The respective criminal provisions must describe the forbidden acts precisely and should avoid vague general clauses. Precise description of illegal acts, without however resorting to a casuistic legislation technique, can easily be achieved, for example, for specific unfair methods of obtaining data or for specific sensitive data. In cases in which precise descriptions of illegal acts are not possible due to the necessity of a difficult balancing of interests (privacy versus freedom of information), criminal law should decline from incriminating substantive infringements of privacy and adopt a formal approach, based on administrative requirements of notification of potentially harmful DP-activities. Failure to comply with these notification requirements and to obey regulations of the data protection authorities could then be subject to sanctions. These formal offences are in accordance with the principle of culpability as long as they can be considered bans *per se* (Gefährdungsdelikte, délits-obstacle), which punish the endangering of privacy rights. In many areas criminal privacy infringements, therefore, would presuppose both the infringement of formal requirements, as well as the endangering of substantive privacy rights (Principle of precision in the wording of criminal law).

(3) The criminalised acts should be described as clearly as possible by the respective penal law provisions. Therefore, a too-extensive use of the referral technique (i.e., the technique pursuant to which activities regulated outside the penal law provisions are criminalised by reference) makes criminal provisions unclear and incomprehensible and should be avoided. If implicit or explicit references of the criminal law are used, the criminal provision itself should at least give an adequate idea of the forbidden acts (Clearness principle).

(4) Different computer-related infringements of privacy should not be criminalised in one global provision. The principle of culpability requires a differentiation according to the interests affected, the acts committed, the status of the perpetrator, as well as of his intended aims and other mental elements (Principle of differentiation).

(5) In principle, computer-related infringements of privacy should only be punishable if the perpetrator acts with intent. Criminalisation of negligent acts should be an exception requiring a special justification (Principle of intent).

(6) Minor computer-related offences against privacy should be punished only in accordance with recommendation No. (87) 18 on the Simplification of Criminal

---

Sieber, Proposal for a Council of Europe Initiative in the Field of Computer-Related Infringements of Privacy, Amendment I, Council of Europe Doc. No. PC-R-CC (86) 33 of 4 December 1986.

Justice, on complaint of the victim or of the Privacy Protection Commissioner or of the Privacy Protection Authority (Principle of complaint)."[400]

Especially due to lack of time, the Committee did not discuss further-going proposals concerning guidelines for national legislators in the field of criminal privacy legislation. However, the above-mentioned proposal of the Council of Europe's Scientific Experts had suggested that first it should be clearly decided if the intention of such guidelines was to create either a "minimum list" (to guarantee a minimum protection of privacy in all Member States), an "optional list" (to illustrate additional acts which might be criminalised in Member States), or a "maximum list" (to prevent over-criminalisation and imprecise criminal laws) and/or a model law. The proposal had especially suggested to concentrate criminal privacy law on the following acts:

"(1) The wilful and illegal disclosure of personal secrets committed by public officials, employees of the PTT services and specific holders of professional secrecy (especially medical personnel, lawyers and bank employees) who have obtained the secrets in the course of professional work;

(2) the wilful and illegal disclosure and/or obtainment of automatically-stored personal data, if this act considerably endangers the privacy rights of an individual and infringes upon the formal notification requirements of privacy legislation or infringes upon a (non-appealable or provisionally enforceable) administrative or court decision;

(3) the wilful and illegal obtainment of automatically-stored personal data by false pretences and/or by infringement of security measures;

(4) the wilful disclosure of incorrect (automatically-stored) personal data (if this act endangers the privacy rights of an individual);

(5) the wilful alteration, storage, erasure and/or suppression of (automatically-stored) personal data committed by unauthorised persons (especially by outside parties) with the intent to cause damage to another party or to gain an illegal profit."[401]

b. United Nations

In 1994, the UN published the "UN Manual on the Prevention and Control of Computer-Related Crime". Among others, the manual contains a chapter on "Substantive Criminal Law Protecting Privacy".[402] The main lines of thinking

400 See Council of Europe, Computer-Related Crime, 1990, pp. 78 et seq.

401 See *Sieber*, Proposal for a Council of Europe Initiative in the Field of Computer-Related Infringements of Privacy, Amendment I, Council of Europe Doc. No. PC-R-CC (86) 33 of 4 December 1986.

402 UN Office at Vienna, International Review of Criminal Policy, UN Manual on the Prevention and Control of Computer-Related Crime, Nos. 43 and 44, 1994, pp. 19 et seq.

in the manual follow the above mentioned proposals of the Council of Europe.[403]

c. Association International de Droit Pénal

The recommendations of the XVth International Congress on Penal Law Section II on Computer Crimes and other Crimes against Information Technology held in Rio de Janeiro, 4-10 September 1994 also contain a chapter on "Specific Issues of Privacy Protection". The chapter is in line with the above-mentioned principles of the Council of Europe and the UN.[404] With respect to privacy protection the recommendations state:

> "12. The significance of protecting privacy interests in the transformed information age against new dangers emanating from the information technology should be recognized. However, the legitimate interests in the free flow and distribution of information within society must also be respected. Privacy interests include the right of citizens to access, by legal means consistent with international human rights, information about themselves which is held by others.
>
> 13. The discussion demonstrated that there are significant differences in opinion as to both the means by, and the degree to which protection should be afforded by administrative, civil, regulatory and criminal law. There are also serious disagreements as to the extent to which criminal law should be involved in the protection of privacy. Therefore, non-penal measures should be given priority, especially where the relations between the parties are governed by contract.
>
> 14. Criminal provisions should only be used where civil law or data protection law do not provide adequate legal remedies. To the extent that criminal sanctions are used, the AIDP notes the basic principles which should be taken into account by states when enacting criminal legislation in this field, as recommended in Recommendation (89) 9 of the Council of Europe. The AIDP proposes further that criminal provisions in the privacy area should in particular:
>
> – be used only in serious cases, especially those involving highly sensitive data or confidential information traditionally protected by law;
> – be defined clearly and precisely rather than by the use of vague or general clauses (Generalklauseln), especially in relation to substantive privacy law;
> – establish a difference between the various levels of gravity of the offenses and to respect the requirements of culpability;
> – be restricted primarily to intentional acts; and
> – permit the prosecution authorities to take into account, in respect of some types of offences, the wishes of the victim regarding prosecution.
>
> 15. Further study should be undertaken to attempt, with special regard to public databases, to define a list of acts which should appropriately be criminalised. This could include intentional acts of infringement of secrecy and serious forms of illegal collection, use, transfer and alteration of personal data which create a danger to personal rights. A starting point for this study might be the tentative proposals that

403 The respective chapter was written by the same expert who had worked for the Council of Europe.

404 Section II of the XVth International Congress on Penal Law was chaired by the same expert who had worked for the Council of Europe.

were considered by the select committee of experts on computer-related crime of the Council of Europe."

d. European Union

The above mentioned 1995 general EC Data Protection Directive[405] addresses criminal law questions only globally. Article 24 of the Directive provides that Member States shall adopt suitable measures to ensure the full implementation of the provisions of the Directive and shall in particular lay down the sanctions to be imposed in case of infringement of the provisions adopted pursuant to the Directive.

B. Economic Criminal Law

The main international activities fighting computer-related economic crime have been undertaken by the OECD and the Council of Europe. However, there are also actions of the European Community, the UN and the Association International de Droit Pénal.

1. Organisation for Economic Co-operation and Development

a. Ad hoc Committee on Computer Crime

The first comprehensive international effort dealing with the criminal law problems of computer crime was initiated by the Organisation for Economic Co-operation and Development (OECD). From 1983 to 1985 an ad hoc committee of the OECD discussed the possibilities of an international harmonisation of criminal laws fighting computer-related economic crime. In September 1985 the Committee recommended that Member States should consider the extent to which knowingly committed acts in the field of computer-related crime should be covered by national penal legislation.

Based on a comparative analysis of substantive law, the ad hoc Committee and the ICCP-Committee of the OECD suggested the following list of acts which could constitute a common denominator for the different approaches taken by Member States:

405 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, OJ L 281/31 of 23.11.1995.

(1) the input, alteration, erasure and/or suppression of computer data and/or computer programs made wilfully with the intent to commit an illegal transfer of funds or of another thing of value;

(2) the input, alteration, erasure and/or suppression of computer data and/or computer programs made wilfully with the intent to commit a forgery;

(3) the input, alteration, erasure and/or suppression of computer data and/or computer programs, or other interference with computer systems, made wilfully with the intent to hinder the functioning of a computer and/or of a telecommunication system;

(4) the infringement of the exclusive right of the owner of a protected computer program with the intent to exploit commercially the program and put it on the market;

(5) the access to or the interception of a computer and/or telecommunication system made knowingly and without the authorisation of the person responsible for the system, either by infringement of security measures or for other dishonest or harmful intentions.[406]

b. Guidelines for the Security of Information Systems

In 1989 the OECD continued its work with special respect to the security of information systems. On 26 November 1992, the Council of the OECD adopted the Recommendation Concerning Guidelines for the Security of Information Systems. The guidelines are addressed to the public and private sectors. They focus on the implementation of minimum standards for the security of information systems. However, they also demand adequate penal, administrative or other sanctions for misuse of information systems, as well as mutual assistance, extradition and other international co-operation in matters relating to the security of information systems.[407]

406 See OECD, Computer-Related Criminality: Analysis of Legal Policy in the OECD-Area, Report DSTI/ICCP 84.22 of 18 April 1986, Final Report (by *Briat* and *Sieber*), pp. 69 et seq.

407 See OECD, Ad Hoc Group of Experts on Information Security, Summary Record of the Meeting of Experts on 5 and 6 March 1990, DSTI/ICCP/90.9 of 19 March 1990; OECD, Ad Hoc Group of Experts on Guidelines for the Security of Information Systems, Summary Record of the First Meeting of Experts, 17 and 18 January 1991, DSTI/ICCP/AH/M (91) 1 of 14 March 1991 and Summary Record of the Second Meeting of Experts, 4 and 5 March 1991, DSTI/ICCP/AH/M (91) 2 of 15 May 1991; OECD, Ad Hoc Group of Experts on Guidelines for the Security of Information Systems, Draft Guidelines for the Security of Information Systems, DSTI/ICCP/AH (90) 21/REV 1 of 31 January 1991; OECD, Guidelines for the Security of Information Systems, 1992, OECD/GD (92) 190. See for the final version of the Guidelines also <http://www.oecd.org/dsti/sti/it/secur/prod/e_secur.htm> (accessed on 24 January 1998).

2. Council of Europe

a. The First Computer Crime Committee and Recommendation No. R (85)

From 1985 to 1989 the Select Committee of Experts on Computer-Related Crime of the Council of Europe discussed the legal problems of computer crime.[408] The Committee elaborated a report which was adopted by the European Committee on Crime Problems at its 38th Plenary Session in June 1989.[409] The work of the Select Committee of Experts on Computer-Related Crime and of the European Committee on Crime Problems prepared Recommendation No. R (89) which was adopted on 13 September 1989 at the meeting of the Ministers' deputies.

This Recommendation suggests that the Member States governments should take into account, when reviewing their legislation or initiating new legislation, the report on computer-related crime and in particular the so-called "guidelines for the national legislatures". These guidelines for national legislatures include a "minimum list" (showing the consensus of the Committee regarding certain computer-related abuses that should be dealt with by criminal law), as well as an "optional list" (describing acts which have already played a practical role in some states, but on which an international consensus for criminalisation could not be reached).

The "minimum list" for offences necessary for uniform criminal policy on legislation concerning computer-related crime enumerates:

> "Computer Fraud": The input, alteration, erasure or suppression of computer data or computer programs, or other interference with the course of data processing, that influences the result of data processing thereby causing economic or possessory loss of property of another person (Alternative draft: with the intent to unlawfully deprive

---

408 In these fields the Council of Europe is upholding an old tradition in the harmonisation of criminal and criminal procedural law. In the present context it might be especially interesting to note that already in 1974, the Standing Committee of the Consultative Assembly of the Council of Europe had adopted a criminal model law on the protection of manufacturing and commercial secrets. (See Consultative Assembly of the Council of Europe, Recommendation 733 (1974) and Resolution 571 (1974) on the protection of manufacturing and commercial secrets). Reference might also be made to the Council of Europe's above mentioned "Recommendation to Member States on Measures to Combat Piracy in the Field of Copyright and Neighbouring Rights", which demands that penalties provided for by legislation in respect to piracy offences should be at an appropriately high level (see infra chapter IV.B.5.e, fn. 380).

409 See Council of Europe, Computer-Related Crime, Recommendation No. R (89) 9, adopted by the Committee of Ministers of the Council of Europe on 13 September 1989 and Report by the European Committee on Crime Problems, Strasbourg 1990; *Csonka*, Council of Europe Activities Related to Information Technology, Data Protection and Computer Crime, 5 (1996) Information & Communications Technology Law, pp. 179 et seq.

that person of his property.) with the intent of procuring an unlawful economic gain for himself or for another person;

"Computer Forgery": The input, alteration, erasure or suppression of computer data or computer programs, or other interference with the course of data processing, in a manner or under such conditions, as prescribed by national law, that it would constitute the offence of forgery if it had been committed with respect to a traditional object of such an offence;

"Damage to Computer Data or Computer Programs": The erasure, damaging, deterioration or suppression of computer data or computer programs without right;

"Computer Sabotage": The input, alteration, erasure or suppression of computer data or computer programs, or interference with computer systems, with the intent to hinder the functioning of a computer or a telecommunication system;

"Unauthorised Access": The access without right to a computer system or network by infringing security measures;

"Unauthorised Interception": The interception, made without right and by technical means, of communications to, from and within a computer system or network;

"Unauthorised Reproduction of a Protected Computer Program": The reproduction, distribution or communication to the public without right of a computer program which is protected by law;

"Unauthorised Reproduction of a Topography": The reproduction without right of a topography protected by law, of a semi-conductor product, or the commercial exploitation or the importation for that purpose, done without right, of a topography or of a semi-conductor product manufactured by using the topography.

The catalogue of the "optional list" contains:

"Alteration of Computer Data or Computer Programs": The alteration of computer data or computer programs without right;

"Computer Espionage": The acquisition by improper means or the disclosure, transfer or use of a trade or commercial secret without right or any other legal justification, with intent either to cause economic loss to the person entitled to the secret or to obtain an unlawful economic advantage for oneself or a third person;

"Unauthorised Use of a Computer": The use of a computer system or network without right, that either: (a) is made with the acceptance of a significant risk of loss being caused to the person entitled to use the system or harm to the system or its functioning, or (b) is made with the intent to cause loss to the person entitled to use the system or harm to the system or its functioning, or (c) causes loss to the person entitled to use the system or harm to the system or its functioning;

"Unauthorised Use of a Protected Computer Program": The use without right of a computer program which is protected by law and which has been reproduced without right, with the intent, either to procure an unlawful economic gain for himself or for another person or to cause harm to the holder of the right."

b. The Two Follow-Up Committees

In the following, the Council of Europe set up two additional select committees dealing with computer crime. The "Committee of Experts on Procedural Law Problems Connected with Computer-Related Crime" (PCPC) was focusing on procedural law issues and will therefore be dealt with infra in chapter IV.E. The "Committee of Experts on Crime in Cyberspace" (PC-

CI) was created in February 1997 and deals with substantive law aspects as well as procedural law questions. The aim of this committee will be to draft binding legal instruments such as a convention. It will also be dealt with infra in chapter IV.E in more detail in connection with procedural law aspects.

3. European Community

a. Legal Advisory Board

The legal questions of computer crime were also discussed by the "Legal Advisory Board" (LAB) of the EC Commission. In December 1987, a first report on "The Legal Aspects of Computer Crime and Security" was delivered to the LAB[410] which discussed it in May 1988.[411] In March 1990 the relevant questions were taken up in a joint conference of the European Commission and of the Council of Europe in Luxembourg. In both meetings, there was a clear support for future international actions of the Council of Europe and the European Community in this field.

b. Council Decisions in the Field of Information Security

In September 1990, the Commission of the European Community published a proposal for a Council Decision in the field of information security, which is part of the above-mentioned six proposals in the field of personal data protection and information security.[412] This proposal included, for a period of two years, an action plan in the field of information security in order to develop a global strategy protecting the users of electronically stored information against accidental or deliberate threats. However, the action plan did not explicitly include criminal law remedies, but comprised the following lines of action:

- development of an information security strategy framework;
- analysis of information security requirements;

410 See *Sieber/Kaspersen/Vandenberghe/Stuurman*, The Legal Aspects of Computer Crime and Security, 1987.

411 See Commission of the European Communities, Directorate-General Telecommunication, Information Industries and Innovation, Legal Advisory Board, Bulletin 88/I and 88/II, as well as the underlying report of *Sieber/Kaspersen/Vandenberghe/Stuurman*, The Legal Aspects of Computer Crime and Security, 1987.

412 See Commission of the European Communities, COM(90) 314 final – SYN 287 and 288 of 13 September 1990. For the other proposals in the field of privacy protection see supra chapter IV.A.1.c.

- solutions for immediate and interim needs;
- specifications, standardisation and verification of information security;
- integration of technological and operational developments for information security within a general strategy; as well as
- integration of certain security functions in information systems.[413]

4. United Nations

In 1990 the legal aspects of computer crime were also discussed by the UN, especially during the Eighth UN Congress on the Prevention of Crime and Treatment of Offenders in Havanna, as well as in the accompanying Symposium on the Prevention and Prosecution of Computer Crime, organised by the Foundation for Responsible Computing. Based on an initiative of the Canadian delegation the Eighth UN Congress on the Prevention of Crime and Treatment of Offenders adopted a resolution which among others:

> "Calls upon Member States, in view of the work already done in the field of computer-related crimes, to intensify their effort to more effectively combat computer abuses that deserve the application of criminal sanctions at the national level, including the consideration, if necessary, of the following measures:
>
> (1) Modernisation of national criminal laws and procedures, including measures to:
>
> (a) Ensure that existing offences and laws concerning investigative powers and admissibility of evidence in judicial proceedings adequately apply and, if necessary, make appropriate changes;
>
> (b) In the absence of laws that adequately apply, create offences and investigative and evidentiary procedures, where necessary, to deal with this novel and sophisticated form of criminal activity;
>
> (c) Provide for the forfeiture or restitution of illegally acquired assets resulting from the commission of computer-related crimes;
>
> (2) Improvement of computer security and prevention measures, taking into account the problems related to the protection of privacy, the respect for human rights and fundamental freedoms and any regulatory mechanisms pertaining to computer usage;
>
> (3) Adoption of measures to sensitise the public, the judiciary and law enforcement agencies to the problem and the importance of preventing computer-related crimes;
>
> (4) Adoption of adequate training measures for judges, officials and agencies responsible for the prevention, investigation, prosecution and adjudication of economic and computer-related crimes,

413 See Commission of the European Communities, COM(90) 314 final – SYN 287 and 288 of 13 September 1990.

(5) Elaboration, in collaboration with interested organisations, of rules of ethics in the use of computers and the teaching of these rules as part of the curriculum and training in informatics;

(6) Adoption of policies for the victims of computer-related crimes which are consistent with the UN Declaration of Basic Principles of Justice for Victims of Crime and Abuse of Power (General Assembly resolution 40/34), including the restitution of illegally obtained assets, and measures to encourage victims to report such crimes to the appropriate authorities."[414]

In late 1990, the Report of the Eighth UN Congress on the Prevention of Crime and the Treatment of Offenders was considered by the Third Committee of the General Assembly. The Third Committee prepared a number of resolutions relating to the report for adoption by the General Assembly. Operative Paragraph 3 of Resolution XV of the Report of the Third Committee "welcomes the instruments and resolutions adopted by the Eighth Congress, and invites Governments to be guided by them in the formulation of appropriate legislation and policy directives ... in accordance with the economic, social, legal, cultural and political circumstances of each country."[415] The General Assembly adopted this resolution on 14 December 1990.

In 1994 the UN published the above-mentioned "Manual on the Prevention and Control of Computer-related Crime" in all official UN languages.[416] The manual examines the phenomenon of computer crime, substantive criminal law protection, procedural law, crime prevention and international co-operation.

In 1997, the UN started to prepare a new manual on crime in Cyberspace. In October/November 1997 the General Conference of UNESCO decided to support a new "Project on ethical, legal and social challenges of the Information Society". It will include legal problems of cyberspace.

5. Association International de Droit Pénal

In 1994, the Association International de Droit Pénal (AIDP) adopted the above-mentioned resolution on computer-related crime.[417] In the field of

414 See UN, Eighth UN Congress on the Prevention of Crime and the Treatment of Offenders, Doc. A/CONF. 144/L. 11 of 4 September 1990, Section 2.

415 See UN General Assembly, Crime Prevention and Criminal Justice Report of the Third Committee, Doc. No. A/45/756 of 7 December 1990, p. 123.

416 See supra IV.A.2.b, fn. 402.

417 See supra IV.A.2.c.

computer-related economic crime, this resolution elaborated some of the points of the Council of Europe's Recommendation No. R (89) 9 and suggested that the list of the Council of Europe required further refinement and the addition of other types of abuse as candidates for criminalisation in the light of advances in information technology.

C. Protection of Intellectual Property

International efforts aiming for a better protection of computer-stored economic values did not start in the field of criminal law, but in the field of civil law. In this area, international action could continue with old traditions in intellectual property protection which had already led to various general agreements (such as the Bern Convention for the Protection of Literary and Artistic Works of 1886, the Universal Copyright Convention of 1952, or the European Patent Convention of 1973). In recent years international efforts especially concern the protection of computer programs, topographies and databases, as well as product piracy.

1. Protection of Computer Programs

a. World Intellectual Property Organisation

The main specifically computer-related efforts in the field of intellectual property protection have dealt with the protection of computer programs. Whether computer programs should be protected by copyright law or by *sui generis* legislation was discussed in particular by the World Intellectual Property Organisation (WIPO) which had, already in 1978, published model provisions for protecting computer programs similar to, but more comprehensive than, copyright protection. The WIPO also proposed a treaty concerning international protection. However, in view of the increasing trend towards copyright protection at the national level, a committee of experts of the WIPO recommended in 1983 that neither a special protection structure nor treaties should be considered at that time, but if necessary, at some later point. During a joint meeting of WIPO/UNESCO held in Geneva in 1985, the majority of participants regarded computer programs as works

which deserve protection by copyright; only a small number of delegations and participants voted for immediate *sui generis* protection.[418]

b. European Community

Other organisations have also devoted great efforts to copyright protection. After a 1989 Commission proposal for a draft EC directive[419] and a 1990 Common Position of the Council,[420] the EC adopted, on 14 May 1991, the Council Directive 91/250/EEC on the legal protection of computer programs.[421] The Council decided to protect of computer programs under copyright law as literary works. Article 1 (3) of the Directive specifies that "a computer program shall be protected if it is original in the sense that it is the author's own intellectual creation" and that "no other criteria shall be applied to determine its eligibility for protection". The directive also regulates who should be protected, which acts should be prohibited, and for how long the protection should last. Article 6 contains a specific exception to decompile a program for the purpose of creating an inter-operable program. The Member States had to implement the Directive before 1 January 1993.

2. Protection of Topographies

A considerable international harmonisation of civil law has also been achieved with regard to the protection of topographies of integrated circuits. Based on a proposal of the EC Commission, the Council enacted a Directive on the legal protection of topographies of semiconductor products in 1986.[422] This Directive has considerably contributed to the harmonisation of the above-mentioned European laws on the protection of the topographies of chip designs.

---

418 See World Intellectual Property Organisation (WIPO), Model Provisions on the Protection of Computer Software, 1978; Copyright, 1989, pp. 146, 149.

419 See Commission of the European Communities, Draft Directive on the Legal Protection of Computer Programs, OJ C 91/4 of 12.04.1989.

420 Common Position of the Council, OJ C 320/22 of 20.12.1990.

421 Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs, OJ L 122/42 of 17.05.1991.

422 Council Directive 87/54/EEC of 16 December 1986 on the legal protection of topographies of semiconductor products, OJ L 24/36 of 27.01.1987.

3. Protection of Databases

a. European Community

On 11 March 1996, the Directive 96/9/EC on the legal protection of databases was finally adopted by the Council.[423] The Directive establishes a new exclusive *sui generis* right for database creators, valid for 15 years, to protect their investment of time, money and effort, irrespective of whether the database is in itself innovative. The Directive will also harmonise copyright law applicable to the structure of databases. Its provisions will apply to both electronic and paper-based databases. It strikes a balance between the interests of the manufacturers of databases and the legitimate interests of their users. Particular attention has been paid to situations in which access to database contents is required for teaching purposes as well as for scientific research.

b. WIPO

WIPO is also active in the field of database protection. The 1996 Diplomatic Conference of WIPO produced a proposal for a treaty on intellectual property with respect to databases. The essence of the proposal was a *sui generis* legal protection of the investment in establishing and marketing databases. In September 1997 the WIPO information meeting on Intellectual Property in Databases in Geneva tolled up the question with respect to providing a *sui generis* protection for databases even if they do not qualify for copyright protection.

4. General Copyright Protection

The protection of intellectual property in computer and communication systems is also influenced by various, more general initiatives in the field of copyright law.

a. European Community

In 1992 and 1993, especially the following Directives have been adopted:

423 The Directive is due to be implemented by Member States no later than 1 January 1998. Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, OJ L 77/20 of 27.03.1996.

- Council Directive 92/100/EEC on rental and lending rights and certain rights relating to copyright;[424]
- Council Directive 93/83/EEC on copyright and rights related to copyright applicable to satellite broadcasting and cable retransmission;[425]
- Council Directive 93/98/EEC on terms of protection of copyright.[426]

Further initiatives of the Commission were described in the Green Paper on copyright and related rights in the information society published by the Commission in July 1995. Following the consultation process of this Green Paper,[427] on 10 December 1997 the Commission adopted a proposal for a European Parliament and Council Directive on the harmonisation of certain aspects of copyright and related rights in the Information Society. The proposed Directive aims to harmonise reproduction rights, rights of communication to the public, and distribution rights as well as exceptions to the restricted acts. It also provides for obligations concerning technological measures and rights management information. As far as "sanctions and remedies" are concerned, Article 8 (1) of the Directive proposal requires that "Member States shall provide appropriate sanctions and remedies in respect of infringements of the rights and obligations set out in this Directive and shall take all the measures necessary to ensure that those sanctions and remedies are applied. The sanctions thus provided for shall be effective, proportionate and dissuasive".

b. World Intellectual Property Organisation

In addition, there are various WIPO initiatives to up-date the copyright framework. Between 1993 and 1995, WIPO held a series of world-wide symposia and fora on the challenges of the new information technologies to copyright. In December 1996, the WIPO diplomatic conference on Certain

---

424 Council Directive 92/100/EEC of 19 November 1992 on rental and lending rights and certain rights relating to copyright, OJ L 346/61 of 27.11.1992.

425 Council Directive 93/83/EEC of 27 September 1993 on copyright and rights related to copyright applicable to satellite broadcasting and cable retransmission, OJ L 248/15 of 06.10.1993.

426 Council Directive 93/98/EEC of 29 October 1993 on terms of protection of copyright, OJ L 290/9 of 24.11.1993.

427 Cf. COM(95) 382. The outcome of a follow-up consultation process on the Green Paper was issued by the Commission on 20 November 1996. Cf. COM(96) 568. The Green Paper and the follow-up Communication address the fundamental question of whether further harmonisation of copyright law is required and if so in what manner. They deal with nine areas of copyright law, including reproduction rights and digital dissemination and transmission rights. The Commission identifies areas where proposals will be made to eliminate significant barriers to trade in copyright goods and services and/or distortions of competition between Member States.

Copyright and Neighbouring Rights Questions adopted the WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT). The treaties contain provisions for copyright protection of copyrightable contents disseminated through global networks. The treaty obliges the contracting parties to provide legal remedies against the circumvention of technological measures (e.g. encryption) used by authors in connection with the exercise of their rights and against the removal of altering information, such as certain data that identify the work of their authors, necessary for the management of their rights.

5. General Product Piracy

Further international initiatives of the Council of Europe, the European Union and the WTO do not specifically aim at computer-stored values, but protect them in a more general context.

a. Council of Europe

Based on the work of the Council of Europe's Steering Committee on the Mass Media, the Committee of Ministers of the Council of Europe adopted the "Recommendation on Measures to Combat Piracy in the Field of Copyright and Neighbouring Rights" in 1988. Among other aspects the recommendation declared that authors of computer software should benefit from copyright protection and suggested both civil and criminal remedies for infringements.[428]

b. European Union

In the European Union, a similar approach was followed by the Council Regulation (EC) No. 3295/94 of 22 December 1994 laying down measures to prohibit the release for free circulation, export, re-export or entry for a suspensive procedure of counterfeit and pirated goods.[429] The Regulation deals with

- definitions especially with respect to counterfeit goods and pirated goods;
- application for action by the custom authorities;

428 See Council of Europe, Recommendation on Measures to Combat Piracy in the Field of Copyright and Neighbouring Rights, Recommendation No. R (88) 2 adopted by the Committee of Ministers of the Council of Europe on 18 January 1988.

429 Council Regulation (EC) No. 3295/94 of 22 December 1994 laying down measures to prohibit the release for free circulation, export, re-export or entry for a suspensive procedure of counterfeit and pirated goods, OJ L 341/8 of 30.12.1994.

- conditions governing action by the customs authorities and by the authorities competent to take a substantive decision;
- provisions applicable to goods found to be counterfeit or pirated goods.

Article 11 of the Regulation requires that "each Member State shall introduce penalties to apply in the event of infringements of Article 2. Such penalties must be sufficiently severe to encourage compliance with the relevant provisions."

c. World Trade Organisation

Trade related aspects of intellectual property rights were especially dealt with by the World Trade Organisation (WTO). The mandate of the WTO includes the Agreement on Trade in Goods (especially GATT), the Agreement on Trade in Services (GATS) as well as the Agreement on Trade-related Aspects of Intellectual Property Rights (TRIPS). The TRIPS Agreement[430] was negotiated in the context of the Uruguay Round in order to reduce distortions and impediments to international trade and to take into account the need to promote effective protection of intellectual property rights. It requires compliance with the substantive provisions of the Bern Convention for Protection of Literary and Artistic Works. With respect to new technologies, the agreement addresses the relevant copyright questions especially relating to computer programs and databases. Section 5 Article 61 of the TRIPS Agreement obliges Member States to provide criminal procedures. It states:

> "Members shall provide for criminal procedures and penalties to be applied at least in cases of wilful trademark counterfeiting or copyright piracy on a commercial scale. Remedies available shall include imprisonment and/or monetary fines sufficient to provide a deterrent, consistently with the level of penalties applied for crimes of a corresponding gravity. In appropriate cases, remedies available shall also include the seizure, forfeiture and destruction of the infringing goods and of any materials and implements the predominant use of which has been in the commission of the offence. Members may provide for criminal procedures and penalties to be applied in other cases of infringement of intellectual property rights, in particular where they are committed wilfully and on a commercial scale."

430 See Bundesgesetzblatt II, 1994, pp. 1565 et seq. (in English), as well as pp. 1730 et seq. (in German).

D. Illegal and Harmful Contents

The centre of activity against illegal and harmful contents in computer networks on the international and supranational level has so far been located at the European Union. However, there are also important initiatives of the Council of Europe, the P8 and the UN.

1. European Union

a. Joint Action of the Council Concerning Racism and Xenophobia

First general – i.e., not computer specific – initiatives against illegal contents have been undertaken by the Council of the European Union. On 15 July 1996, based on Article K.3 EU Treaty, the Council adopted a "joint action to combat racism and xenophobia".[431] Title 1 (A and B) of the Joint Action provide:

> "A. In the interests of combating racism and xenophobia, each Member State shall undertake, in accordance with the procedure laid down in Title II, to ensure effective judicial co-operation in respect of offences based on the following types of behaviour, and, if necessary for the purposes of that co-operation, either to take steps to see that such behaviour is punishable as a criminal offence or, failing that, and pending the adoption of any necessary provisions, to derogate from the principle of double criminality for such behaviour:
>
> (a) public incitement to discrimination, violence or racial hatred in respect of a group of persons or a member of such a group defined by reference to colour, race, religion or national or ethnic origin;
>
> (b) public condoning, for a racist or xenophobic purpose, of crimes against humanity and human rights violations;
>
> (c) public denial of the crimes defined in Article 6 of the Charter of the International Military Tribunal appended to the London Agreement of 8 April 1945 insofar as it includes behaviour which is contemptuous of, or degrading to, a group of persons defined by reference to colour, race, religion or national or ethnic origin;
>
> (d) public dissemination or distribution of tracts, pictures or other material containing expressions of racism and xenophobia;
>
> (e) participation in the activities of groups, organisations or associations, which involve discrimination, violence, or racial, ethnic or religious hatred.
>
> B. In the case of investigations into, and/or proceedings against, offences based on the types of behaviour listed in paragraph A, each Member State shall, in accordance with Title II, improve judicial co-operation in the following areas and take appropriate measures for:

431 OJ L 185/5 of 24.07.1996.

(a) seizure and confiscation of tracts, pictures or other material containing expressions of racism and xenophobia intended for public dissemination, where such material is offered to the public in the territory of a Member State;

(b) acknowledgement that the types of behaviour listed in paragraph A should not be regarded as political offences justifying refusal to comply with requests for mutual legal assistance;

(c) providing information to another Member State to enable that Member State to initiate, in accordance with its law, legal proceedings or proceedings for confiscation in cases where it appears that tracts, pictures or other material containing expressions of racism and xenophobia are being stored in a Member State for the purposes of distribution or dissemination in another Member State;

(d) the establishment of contact points in the Member States which would be responsible for collecting and exchanging any information which might be useful for investigations and proceedings against offences based on the types of behaviour listed in paragraph A."

b. Activities of the Council with Respect to the Internet

The specific issue of illegal and harmful content on the Internet was discussed at the informal Council meeting held in Bologna on 24 April 1996. The European Telecommunications Ministers and Culture Ministers asked the Commission to produce a problem analysis assessing the desirability of European or international regulations. Furthermore, at the end of September 1996 various Council sessions considered the relevant questions: The informal meeting of Ministers of Justice and Home Affairs in September 1996 in Dublin discussed co-operation between Member States to combat trade in human beings and sexual abuse of children. The Ministers of Cultural and Audiovisual meeting in Galway in September 1996 welcomed the announcement of a Green Paper on the protection of minors and human dignity. The meeting of the Council of Telecommunications Ministers in September 1996, following the informal Bologna Council, discussed questions of preventing the dissemination of illegal material on the Internet. The Council also requested a Working Party on illegal and harmful contents on the Internet to present concrete proposals for possible measures to combat the illegal use of the Internet.

On 17 February 1997, the Telecommunications Council formally adopted a Resolution on illegal and harmful content on the Internet.[432] In this Resolution the Council and the representatives of the governments of the Member States

432 Resolution of the Council and of the Representatives of the Governments of the Member States, meeting within the Council on illegal and harmful content on the Internet, OJ C 70/1 of 06.03.1997.

"4. invite the Member States to start with the following measures:

encourage and facilitate self-regulatory systems including representative bodies for Internet service providers and users, effective codes of conduct and possibly hot-line reporting mechanisms available to the public;

encourage the provision to users of filtering mechanisms and the setting up of rating systems; for example the PICS (platform for internet content selection) standard launched by the international World-Wide-Web consortium with Community support should be promoted;

participate actively in the International Ministerial Conference to be hosted by Germany and encourage attendance by representatives of the actors concerned;

5. request the Commission, as far as Community competences are concerned, to:

ensure the follow-up and the coherence of work on the measures suggested in the above mentioned report, taking into account other relevant work in this field and to reconvene the Working Party as necessary to monitor progress and take further initiatives if appropriate;

foster co-ordination at Community level of self-regulatory and representative bodies;

promote and facilitate the exchange of information on best practice in this area;

foster research into technical issues, in particular filtering, rating, tracing and privacy-enhancing, taking into account Europe's cultural and linguistic diversity;

consider further the question of legal liability for Internet content;

6. recommend that the Commission, in the framework of Community competences, and Member States take all necessary steps to enhance the effectiveness of the measures referred to in this resolution through international co-operation building on the results of the International Ministerial Conference and in discussions in other international forums."

c. Activities of the European Commission

With respect to finding solutions to these new issues, the EC Commission has also published several documents: These are the Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions on illegal and harmful content on the Internet of 16 October 1996,[433] the Green Paper on the Protection of Minors and Human Dignity on Audiovisual and Information Services of 16 October 1996,[434] the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions on an Action Plan on promoting safe use

433 Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions on illegal and harmful content on the Internet of 16 October 1996, COM(96) 0487. See also in this context European Commission (DG XIII), Interim report on Initiatives in EU Member States with respect to Combating Illegal and Harmful Content on the Internet, WPIC 16/97, Version 7 of 4 June 1997.

434 COM(96) 0483.

of the Internet adopted by the Commission on 26 November 1997 as well as a Council Recommendation on the Protection of Minors and Human Dignity.

The Communication on illegal and harmful content on the Internet confirms that all persons involved in the Internet (authors, content provider, host service providers, network operators, access providers and users) are subject to the respective laws of the Member States and do not operate in a legal vacuum. The paper identifies different variations of illegal and harmful content and gives policy option for EU action. As a first set of measures to combat the source of illegal content the Commission proposes co-operation in the context of justice and home affairs between Member States by exchanging information on those providing criminal content and through defining minimum European standards in criminal content, developing a European framework to clarify the administrative rules and regulations governing the liability of access providers and host service providers, as well as strengthening the process of self-regulation through co-operation between associations of Internet access providers and research to find technological solutions for limiting the distribution of illegal content. With regard to harmful contents, the Communication suggests encouraging the use of filtering software such as PICS and for developing European rating systems, inviting content producers to adopt codes of conduct to content published on the Internet, including systematic self-rating of content, as well as launching national awareness actions for parents and teachers.

The Green Paper on the Protection of Minors and Human Dignity is looking beyond these initial short term measures. The Green Paper deals with the specific and fundamental issues of the fight against the dissemination of content offensive to human dignity and the protection of minors against exposure to content that is harmful to their development. The Green Paper proposes ten basic questions to help create the conditions for the establishment of a coherent framework for the protection of minors and human dignity for the "information age".

In the Action Plan on promoting safe use of the Internet, the Commission identified areas where concrete measures are needed and where Community resources should be made available in order to encourage an environment favourable to the development of the Internet industry. These areas are the promotion of self-regulation and creation of content-monitoring schemes including an European network of hot-lines, the demonstration and application of effective filtering services and compatible rating systems, and the promotion of awareness actions directed at users, in particular children, parents and teachers. The proposed Action Plan is specifically aimed at actions where financial support from the Community is necessary. It aims to incite the actors (industry, users) to develop and implement adequate systems of self regulation, to pump prime developments by supporting demonstrations and stimulating application of technical solution, alert and inform parents and teachers, foster co-operation and exchange of experiences and best practices, promote co-ordination across Europe and between actors concerned, and ensure compatibility between the approach taken in Europe and elsewhere. The Action Plan comprises four concrete action lines for creating a safe environment, for developing filtering and rating systems, for encouraging awareness actions, and for support measures.

Contrary to the action line, the Council Recommendation on the Protection of Minors and Human Dignity is of a legal nature and aims to promote common guidelines for the implementation of a framework for self-regulation to protect minors and human dignity in audiovisual and information services.

d. European Parliament

On 24 April 1997, the European Parliament adopted a Resolution on the Commission's communication on illegal and harmful content on the Internet,[435] supporting the initiatives undertaken by the Commission and stressing the need for international co-operation in various areas, to be initiated by the Commission.

In addition, the European Parliament published a study on the "Feasibility of censoring and jamming pornography and racism in informatics" produced by Scientific and Technological Options Assessment (STOA).[436] The report concentrates on technical questions and possibilities of blocking illegal and harmful contents.

e. Other Activities

Issues of illegal and harmful contents were also dealt with at the Ministerial Conference on "Global Information Networks" which in July 1997 was jointly organised by the European Union and the German government. The conference produced three declarations of Ministers, of industry and of users. With respect to responsibility for illegal contents the declaration of Ministers stresses that there should be no active control of content of third parties and that network and access providers should in general not be responsible for contents.[437]

2. P8 Countries

a. P8 Expert Group on "Misuse of International Data Networks"

The P8 expert group on "Misuse of International Data Networks" was established by the Ministers and Chief Advisors of Science of the G7 countries, Russia and the European Union (Carnegie-Group) in 1996. It consisted of legal and technical experts of the Member States in the field of international computer networks. The expert groups mandate was to evaluate the misuse of international data networks and to suggest recommendations for potential solutions. The expert group held three

435 COM(96) 0487 – C4-0592/96, <http://www.europarl.eu.int/dg1/a4/en/a4-97/a4-0098.htm> (accessed on 24 January 1998).

436 See European Parliament, STOA, Feasibility of censoring and jamming pornography and racism in informatics, Draft Final Report, May 1997.

437 See Global Information Networks, Ministerial Conference Bonn 6–8 July 1997, Ministererklärung, p. 7 Nos. 41 and 42.

meetings in Bonn, November 1996, in Paris, June 1997 and in Rome, October 1997. The group presented its report to the Carnegie-Group at their meeting at Montebello/Canada on 5-7 December 1997.

The report emphasises the broad scale of the outstanding benefits and promises of the Internet for practically all sectors of public, political and commercial process of communication and – not least – for the individual life of private persons and groups. It underlines, however, that the full use of benefits will depend – to a great deal – on the avoidance or at least minimisation of the various possibilities of misuse. Analysing the situation, the report identifies two areas of misuse: (1) illegal or harmful actions, where the Internet is used in order to engage in illegal activities, as well as (2) illegal or harmful actions, where the Internet is used to transfer illegal information to users.

In order to find appropriate answers to these challenges, the report clusters the potential solutions into four approaches of activities, aiming at developing practical steps for improving the proper use and overall acceptance of new communication technologies and services. These four areas are: (1) awareness and education, (2) technology, (3) information and communications industry, as well as (4) legal measures. The report suggests to develop, as a first step, concise sets of solutions along and across these four areas. Consequently, the expert group submitted a number of recommendations.[438]

b. P8 Subgroup on High Tech Crime

The P8 countries also work together in the P8 subgroup on high tech crime. Since this subgroup on high tech crime is concentrating on procedural law questions and practical prosecution of computer crime their activities are dealt with infra E.3 in the context of procedural law questions.

3. Organisation for Economic Co-operation and Development

Initiatives on illegal and harmful contents on the Internet were also started by the OECD within its Committee for Information, Computer and

438 These recommendations are mentioned infra chapter V.B with respect to future solutions suggested by this study. The author of this study has been the chairman of the first meeting of the expert group of "Misuse of International Data Networks" and a co-editor of the expert groups report. He fully supports the solutions also with respect to the European Union; for these reasons the expert groups' recommendations are very similar to the author's suggestions.

Communications Policy (ICCP-committee). In October 1996 the French and subsequently also the Belgian government proposed to the OECD an agreement on international co-operation with regard to the Internet (Charte de coopération internationale sur Internet – Projet de la contribution française en vue des travaux préparatoires à une Conférence ministérielle de l'OCDE). The document comprises three parts: First it lays down a number of principles approved by the signatories (typology of the players, rules to be applied, principles concerning the liability of publishers and host service providers). Secondly, it sets out a list of guidelines aimed in particular at guaranteeing the respect of basic ethical rules and improving consumer protection. Finally, the document sets forth the principles of judicial and police co-operation between the signatories.

In February 1997 the ICCP Committee agreed to undertake a study aimed at reviewing the existing legislations and practices in Member States concerning the Internet. The study is expected to be submitted to the ICCP Committee in late 1997.

4. United Nations

The UN have contributed especially to childrens' rights. On 20 November 1989, the General Assembly of the UN adopted the Convention on the Rights of the Child. The UN have also supported the World Congress Against Commercial Sexual Exploitation of Children on 5 June 1997.[439]

E. Criminal Procedural Law

In the field of procedural law international action has already started in all of the above described areas and concerns: the field of coercive powers, the legality of processing personal data in the course of criminal proceedings, and the admissibility of computer-generated evidence in court proceedings. The focus of attention has been on coercive powers as well as on co-operation in criminal matters. The main actors in this field have been the Council of Europe, the European Union, the P8 and Interpol.

439 Cf. for more details <http://www.hartford-hwp.com/archives/28/024.html> (accessed on 28 January 1998).

1. Council of Europe

a. The European Convention for the Protection of Human Rights and Fundamental Freedoms

An early international harmonisation of the above mentioned coercive powers in the field of information technology derived from the European Convention for the Protection of Human Rights and Fundamental Freedoms. Article 8 of the Convention guarantees that "everyone has the right to respect for his private and family life, his home and his correspondence" (Subsection 1) and that "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" (Subsection 2).[440]

The European Court of Human Rights applied these guarantees especially in the area of wiretapping.[441] In the "Klass"-case[442], the court confirmed the legality of the German "Law on Limitations of the Secrecy of Letters, Post and Telecommunication"[443] which, under specific conditions, provides the authorities with the competence to supervise postal services and to wiretap telephone communications. However, the court stated that the exemption clause of Article 8 (2) of the Convention should be interpreted narrowly, that any system of surveillance has to include effective guarantees against abuses, and that any infringement of civil liberties by public authorities must be subject to independent control (preferably by an independent judge).[444] In the "Malone"-case[445] the court

440 See also Article 12 of the Universal Declaration of Human Rights, adopted and proclaimed by General Assembly Resolution 217 (III) A of 10 December 1948: "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."

441 With respect to telephone tapping, the Council of Europe in May 1982 also published a study on "Telephone Tapping and the Recording of Telecommunications in Some Council of Europe Member States". The aim of the publication was to provide countries, wishing to introduce new legislation, with a comparative outline of the approaches adopted in the various Member States. See Council of Europe, Legislative Dossier No. 2, "Telephone Tapping and the Recording of Telecommunications in Some Council of Europe Member States", Strasbourg, May 1982.

442 Decision of the European Court of Human Rights of 6 September 1978, (1979) Europäische Grundrechte Zeitschrift, pp. 278 et seq.

443 Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses of 13 August 1968 (G 10–Gesetz).

444 For the latter requirement see also Articles 6 (1) and 13 of the Convention.

had to decide on the interception of communication, which at that time was practised in the United Kingdom by the police without specific legal justification. It confirmed the principle (developed in more detail in the Sunday-Times-decision)[446] that the convention's term "in accordance with the law" ("prévue par la loi") does not only comprehend statutory provisions, but also includes unwritten (common) law. However, the Court stressed that the legal requirements for an interception must be formulated with sufficient precision in order to be foreseeable by the citizens and to avoid arbitrary acts by the authorities. The Court considered the law of England and Wales concerning the interception of communication was unclear and that it did not fulfil these requirements.

b. The First Computer Crime Committee and Recommendation No. R (85) S

A more general discussion of coercive powers in the field of information technology was held by the above mentioned Committee of Experts on Computer-Related Crime of the Council of Europe which primarily dealt with substantive law questions.[447] In its final report the Committee and the Council of Europe's Committee on Crime Problems recommended that in the future, consideration should be given to the respective questions either in a computer-specific context or in the context of a more general harmonisation of the various national coercive powers. In the long run harmonisation of coercive powers and of the respective legal safeguards should promote international legal co-operation in all fields.

c. The Second Computer Crime Committee and Recommendation No. R (95) 13

Two years after the adoption by the Committee of Ministers of Recommendation No. R (89) 9 on computer-related crime a new select Committee of Experts on Procedural Law Problems Connected with Computer-related Crime" (PC-PC) was set up at the Council of Europe in 1991. The Committee completed its work in April 1995 by adopting a draft recommendation and a draft explanatory report relating thereto. The draft

445 Decision of the European Court of Human Rights of 2 August 1984, (1985) Europäische Grundrechte Zeitschrift, pp. 17 et seq. As a consequence of the decision, the plaintiff received compensation from the Government, see Decision of the European Court of Human Rights, (1985) Europäische Grundrechte Zeitschrift, pp. 677 et seq.

446 Decision of the European Court of Human Rights of 26 April 1979, (1979) Europäische Grundrechte Zeitschrift, pp. 386 et seq., at 397. Article 10 (2) of the Convention requires interference with the freedom of expression to be "prescribed by law" ("prévue par la loi").

447 See supra chapter IV.B.2.b.

recommendation and the draft explanatory report were adopted by the Committee of Ministers of the Council of Europe on 11 September 1995 in Recommendation No. R (95) 13.[448]

Recommendation No. R (95) 13 of the Committee of Ministers to Member States concerning problems of criminal procedural law connected with information technology recommends the governments of the Member States, when reviewing their internal legislation and practice, to be guided by the principles appended to the recommendation and to ensure publicity for these principles. The appendix to the recommendation suggests:

"I. Search and seizure

1. The legal distinction between searching computer systems and seizing data stored therein and intercepting data in the course of transmission should be clearly delineated and applied.
2. Criminal procedural laws should permit investigating authorities to search computer systems and seize data under similar conditions as under traditional powers of search and seizure. The person in charge of the system should be informed that the system has been searched and of the kind of data that has been seized. The legal remedies that are provided for in general against search and seizure should be equally applicable in case of search in computer systems and in case of seizure of data therein.
3. During the execution of a search, investigating authorities should have the power, subject to appropriate safeguards, to extend the search to other computer systems within their jurisdiction which are connected by means of a network and to seize the data therein, provided that immediate action is required.
4. Where automatically processed data is functionally equivalent to a traditional document, provisions in the criminal procedural law relating to search and seizure of documents should apply equally to it.

II. Technical surveillance

5. In view of the convergence of information technology and telecommunications, laws pertaining to technical surveillance for the purposes of criminal investigations, such as interception of telecommunications, should be reviewed and amended, where necessary, to ensure their applicability.
6. The law should permit investigating authorities to avail themselves of all necessary technical measures that enable the collection of traffic data in the investigation of crimes.
7. When collected in the course of a criminal investigations and in particular when obtained by means of intercepting telecommunications, data which is the object of legal protection and processed by a computer system should be secured in an appropriate manner.
8. Criminal procedural laws should be reviewed with a view to making possible the interception of telecommunications and the collection of traffic data in the investigation of serious offences against the confidentiality, integrity and availability of telecommunication or computer systems.

448 See also *Csonka*, Council of Europe Activities Related to Information Technology, Data Protection and Computer Crime, 5 (1996) Information & Communications Technology Law, pp. 186 et seq.

III. Obligations to co-operate with the investigating authorities

9. Subject to legal privileges or protection, most legal systems permit investigating authorities to order persons to hand over objects under their control that are required to serve as evidence. In a parallel fashion, provisions should be made for the power to order persons to submit any specified data under their control in a computer system in the form required by the investigating authority.

10. Subject to legal privileges or protection, investigating authorities should have the power to order persons who have data in a computer system under their control to provide all necessary information to enable access to a computer system and the data therein. Criminal procedural law should ensure that a similar order can be given to other persons who have knowledge about the functioning of the computer system or measures applied to secure the data therein.

11. Specific obligations should be imposed on operators of public and private networks that offer telecommunication services to the public to avail themselves of all necessary technical measures that enable the interception of telecommunications by the investigating authorities.

12. Specific obligations should be imposed on service-providers who offer telecommunication services to the public, either through public or private networks, to provide information to identify the user, when so ordered by the competent investigating authority.

IV. Electronic evidence

13. The common need to collect, preserve and present electronic evidence in ways that best ensure and reflect their integrity and irrefutable authenticity, both for the purposes of domestic prosecution and international co-operation, should be recognised. Therefore, procedures and technical methods for handling electronic evidence should be further developed, and particularly in such a way as to ensure their compatibility between states. Criminal procedural law provisions on evidence relating to traditional documents should similarly apply to data stored in a computer system.

V. Use of encryption

14. Measures should be considered to minimise the negative effects of the use of cryptography on the investigation of criminal offences, without affecting its legitimate use more than is strictly necessary.

VI. Research, statistics and training

15. The risks involved in the development and application of information technology with regard to the commission of criminal offences should be assessed continuously. In order to enable the competent authorities to keep abreast of new phenomena in the field of computer-related offences and to develop appropriate counter-measures, the collection and analysis of data on these offences, including the modus operandi and technical aspects, should be furthered.

16. The establishment of specialised units for the investigation of offences, the combating of which requires special expertise in information technology, should be considered. Training programmes enabling criminal justice personnel to avail themselves of expertise in this field should be furthered.

VII. International co-operation

17. The power to extend a search to other computer systems should also be applicable when the system is located in a foreign jurisdiction, provided that immediate action is required. In order to avoid possible violations of state sovereignty or international law, an unambiguous legal basis for such extended search and seizure should be established. Therefore, there is an urgent need for

negotiating international agreements as to how, when and to what extent such search and seizure should be permitted.

18. Expedited and adequate procedures as well as system of liaison should be available according to which the investigating authorities may request the foreign authorities to promptly collect evidence. For that purpose the requested authorities should be authorised to search a computer system and seize data with a view to its subsequent transfer. The requested authorities should also be authorised to provide trafficking data related to a specific telecommunication, intercept a specific telecommunication or identify its source. For that purpose, the existing mutual legal assistance instruments need to be supplemented."

d. The Third Computer Crime Committee on Crime in Cyberspace

In February 1997 the European Committee on Crime Problems (CDPC) set up a new "Committee of Experts on Crime in Cyberspace" (PC-CY). The Committee's terms of reference are to examine problems of criminal law connected with information technology, in particular

- cyberspace offences and other substantive criminal law issues where a common approach may be necessary for the purposes of international co-operation;
- the use, including the possibility of transborder use, and the applicability of coercive powers in a technological environment;
- the question of jurisdiction in relation to information technology offences;
- questions of international co-operation in the investigation of cyberspace offences.

The Committee had its first meeting in 1997. It intends to prepare a binding convention on substantive as well as on procedural computer-related law.

2. European Union

Within the European Union, activities in the field of procedural law have not been undertaken under the so-called first pillar, but under the third pillar,[449] i.e. intergovernmental co-operation in matters of home affairs institutionalised by the K-Articles of the Treaty on European Union (the Maastricht Treaty).

449 For the underlying reasons and competences see infra chapter VI.

a. Council Resolution on Interception of Telecommunications

On 17 January 1995, based on Articles K.1 (9) and K.2 (2) of the Treaty on European Union, the Council of the European Union adopted a Resolution on the international requirements for a lawful interception of telecommunications.[450] The Council noted that the requirements of Member States to enable them to conduct lawful interception of telecommunications, annexed to the resolution ("the Requirements"), constitute an important summary of the needs of the competent authorities for the technical implementation of legally authorised interception in modern telecommunications systems. The Council considered that these requirements should be taken into account by the Member States as follows:

"1. Law enforcement agencies require access to the entire telecommunications transmitted, or caused to be transmitted, to and from the number or other identifier of the target service used by the interception subject. Law enforcement agencies also require access to the call-associated data that are generated to process the call. ...

2. Law enforcement agencies require a real-time, full-time monitoring capability for the interception of telecommunications. Call associated data should also be provided in real-time. If call associated data cannot be made available in real time, law enforcement agencies require the data to be available as soon as possible upon call termination.

3. Law enforcement agencies require network operators/service providers to provide one or several interfaces from which the intercepted communications can be transmitted to the law enforcement monitoring facility. These interfaces have to be commonly agreed on by the interception authorities and the network operators/service providers. Other issues associated with these interfaces will be handled according to accepted practices in individual countries. ...

4. Law enforcement agencies require interceptions to be implemented so that neither the interception target nor any other unauthorised person is aware of any changes made to fulfil the interception order. In particular, the operation of the target service must appear unchanged to the interception subject.

5. Law enforcement agencies require the interception to be designed and implemented to preclude unauthorised or improper use and to safeguard the information related to the interception. ...

6. Based on a lawful enquiry and before implementation of the interception, law enforcement agencies require (1) the interception subject's identity, service number or other distinctive identifier, (2) information on the services and features of the telecommunications system used by the interception subject and delivered by network operators/service providers, and (3) information on the technical parameters of the transmission to the law enforcement monitoring facility.

7. During the interception, law enforcement agencies may require information and/or assistance from the network operators/service providers to ensure that the communications acquired at the interception interface are those communications

450 OJ C 329/1 of 04.11.1996.

associated with the target service. The type of information and/or assistance required will vary according to the accepted practices in individual countries.

8. Law enforcement agencies require network operators/service providers to make provisions for implementing a number of simultaneous incepts. Multiple interceptions may be required for a single target service to allow monitoring by more than one law enforcement agency. In this case, network operators/service providers should take precautions to safeguard the identities of the monitoring agencies and ensure the confidentiality of the investigations. The maximum number of simultaneous interceptions for a given subscriber population will be in accordance with national requirements.
9. Law enforcement agencies require network operators/service providers to implement interceptions as quickly as possible (in urgent cases within a few hours or minutes). The response requirements of law enforcement agencies will vary by country and by the type of target service to be intercepted.
10. For the duration of the interception, law enforcement agencies require that the reliability of the services supporting interceptions at least equals the reliability of the target services provided to the interception subject. Law enforcement require the quality of service of the intercepted transmissions forwarded to the monitoring facility to comply with the performance standards of the network operators/service providers."

b. Group K4 on Police Co-operation

The aforementioned Council Resolution on the international requirements for the lawful interception of telecommunications was especially promoted by the Council group K4 on Police Co-operation which was established under the Maastricht Treaty and which meets approximately every six weeks in Brussels. The group discusses common problems of telecommunication surveillance with the aim of finding solutions of the EU as a whole and of promoting these solutions in negotiations with telecommunications industry and institutions responsible for technical and legal standards. In April 1997 the group was especially dealing with questions of supervision of Internet communication.

c. Working Party on Mutual Assistance

The EU Working Party on Mutual Assistance in Criminal Matters is presently also addressing the issue of interception of telecommunication systems outside national boundaries, especially with respect to the international interception of satellite personal communication systems.

d. International Law Enforcement Telecommunications Seminar

Following the establishment of contacts with countries outside the EU (particularly with the US) in 1992/1993 an expert group "International Law Enforcement Telecommunications Seminar – ILETS" was formed as outgrowth of the expert group on legal question regarding telecommunications surveillance (originally within the framework of TREVI).

The aim of the group is to ensure the legality of telecommunications surveillance in modern telecommunication networks in accordance with respective national laws in the interest of criminal prosecution and national security. So far the efforts of the group concentrated on surveillance of mobile telephones and future satellite networks.

e. Action Plan to Combat Organised Crime

On 28 April 1997, the Council adopted, under title VI of the EU Treaty, the "Action Plan to Combat Organised Crime".[451] The action plan has been elaborated by the High Level Group, created by the Council (Dublin, 13, 14 December 1996), and tasked to examine the fight against organised crime in all its aspects. The action plan to combat organised crime contains 15 political guidelines and 30 specific recommendations, together with the proposed time-table and an indication of where the responsibility for implementation of each recommendation might be considered to lay.

No. 15 of the political guidelines and – in more detail – No. 5 of the specific recommendations specifically call for a cross-pillar study:

> "A cross-pillar study on high-technology crime and its use and links with organized crime should be carried out within the Union (see political guideline No. 15). This study should pave the way for a policy ensuring an efficient public protection. While avoiding undue restrictions, law enforcement and judicial authorities should have the means, as a complement to the specific responsibility incumbent on the technology and service-providers, to prevent and combat the misuse of these new technologies. Attention should be paid both to illegal practices (such as the use of these technologies by criminal organisations to facilitate their activities) or illegal contents (such as child pornography or dissemination of synthetic drug recipes)."

3. P8 Subgroup on High-Tech Crime

With respect to criminal matters the P8 countries[452] work on two major initiatives, focusing on terrorism and transnational organised crime. In the area of transnational organised crime, in 1996 the P8 senior experts group on transnational crime (which at that time was called the Lyon group) decided to create several subgroups. Since that time subgroup V is dealing with high tech crime. So far the subgroup had meetings in Chantilly/Virginia in January 1997, in London in June/July 1997 and in Washington D.C. in

451 See OJ C 251/1 of 15.08.1997.

452 The P8 Group evolved when Russia joined the Group of Seven (or G7 Countries: Canada, France, Germany, Italy, Japan, United Kingdom and the United States of America) and those nations adopted an agenda that reached beyond the historically economic focus of the G7 in order to address political and global issues.

December 1997. The main focus of the subgroup is on the issues of procedural law, international co-operation and effective prosecution of computer crimes. Topics discussed are e.g.

- comparison and harmonisation of countries' substantive laws,
- real-time trap and trace,
- locating people in a wireless environment,
- international co-operation in the collection of evidence,
- computer searches/forensics,
- encryption,
- comprehensive international training,
- international high-tech contacts.

In the meeting of Justice and Interior Ministers of the Eight in December 1997 in Washington D.C., the following statement of principles was agreed upon:

"I. There must be no save havens for those who abuse information technologies.

II. Investigation and prosecution of international high-tech crimes must be coordinated among all concerned States, regardless of where harm has occurred.

III. Law enforcement personnel must be trained and equipped to address high-tech crimes.

IV. Legal systems must protect the confidentiality, integrity, and availability of data and systems from unauthorized impairment and ensure that serious abuse is penalized.

V. Legal systems should permit the preservation of and quick access to electronic data, which are often critical to the successful investigation of crime.

VI. Mutual assistance regimes must ensure the timely gathering and exchange of evidence in cases involving international high-tech crime.

VII. Transborder electronic access by law enforcement to publicly available (open source) information does not require authorization from the State where the data resides.

VIII. Forensic standards for retrieving and authenticating electronic data for use in criminal investigations and prosecutions must be developed and employed.

IX. To the extent practicable, information and telecommunications systems should be designed to help prevent and detect network abuse, and should also facilitate the tracing of criminals and the collection of evidence.

X. Work in this area should be coordinated with the work of other relevant international fora to ensure against duplication of efforts."

In support of these principles, the Ministers adopted an action plan, in order to direct their officials to

"1. Use our established network of knowledgeable personnel to ensure a timely, effective response to transnational high-tech cases and designate a point-of-contact who is available on a twenty-four hour basis.

2. Take appropriate steps to ensure that a sufficient number of trained and equipped law enforcement personnel are allocated to the task of combating high-tech crime and assisting law enforcement agencies of other States.

3. Review our legal systems to ensure that they appropriately criminalize abuses of telecommunications and computer systems and promote the investigation of high-tech crimes.
4. Consider issues raised by high-tech crimes, where relevant, when negotiating mutual assistance agreements or arrangements.
5. Continue to examine and develop workable solutions regarding: the preservation of evidence prior to the execution of a request for mutual assistance; transborder searches of data where the location of that data is unknown.
6. Develop expedited procedures for obtaining traffic data from all communications carriers in the chain of a communication and to study ways to expedite the passing of this data internationally.
7. Work jointly with industry to ensure that new technologies facilitate our effort to combat high-tech crime
8. Ensure that we can, in urgent and appropriate cases, accept and respond to mutual assistance requests relating to high-tech crime by expedited but reliable means of communications, including voice, fax, or e-mail, with written confirmation to follow where required.
9. Encourage internationally recognized standards-making bodies in the fields of telecommunications and information technologies to continue providing the public and private sectors with standards for reliable and secure telecommunications and data processing technologies.
10. Develop and employ compatible forensic standards for retrieving and authenticating electronic data for use in criminal investigations and prosecutions."

4. Interpol

Interpol held a first international conference on computer crime in Lyon in April 1995. The conference recommended that the problem of computer-related crime should be addressed similarly in each of the Interpol Member States and in the African, American and Asian regions. A steering committee was suggested to promote and co-ordinate these regional initiatives.

Today, the ICPO/Interpol "Standing Committee on Information Technology" is consisting of ICPO/Interpol representatives from Europe, the United States of America, Asia, South America and Africa. It is analysing information and communication technology in ICPO/Interpol countries. The group holds one or two meetings per year.

On the occasion of the 1990 European Regional Conference in Budapest, the Technical Committee for Co-operation in Europe was requested to establish an expert task group on the prevention and control of computer crime. At the 59th General Meeting in Ottawa the European Regional Group achieved agreement for the establishment of a "Computer Crime" task group.

The task group held various meetings in three working subgroups.[453] Delegates of the task group are police and computer experts of European Countries. The task force organised various training courses (starting with a course at the University of Würzburg/Germany) and published a handbook on "Prevention and Control of Computer Crime/Crime Involving Computers".[454]

5. International Organisation on Computer Evidence

The task group "International Organisation on Computer Evidence" was established on an initiative of the FBI Computer Analysis and Response Team (CART). It comprises participants from Europe, the United States of America, Canada, South Africa and Asia.

The groups objective is to exchange information, suitable software and hardware, methods of criminal investigations as well as the testing of analytical and investigative tools for achieving international standardisation.

6. NATO: Allied Command Europe Counterintelligence Activity

Police and counterintelligence representatives from NATO are meeting annually for a conference in order to exchange information and experience relating to crimes involving communication and information technology, especially cases of computer espionage and computer crime from the standpoint of national security.[455] Knowledge is also shared in the areas of cryptography and technical resources to investigations.

453 SG 1: Computer Viruses Bulletin Board, Mobile Telecommunication, et al; SG 2: Training and legislation; SG 3: Methods of Prevention and Control

454 See International Criminal Police Organisation Interpol (ed.), Computers and Crime, and e.g. in Germany Bundeskriminalamt – Nationales Zentralbüro der IKPO-Interpol für die Bundesrepublik Deutschland (ed.), Computer und Kriminalität (brochure not dated).

455 See, e.g., the LATE GAMBIT-Conference 1996.

F. Regulations on Protection Measures

1. Obligations for Security Measures

On the European level, a duty to implement safety measures mainly results from Article 17 of the above-mentioned Directive 95/46/EC on Data Protection, which expressly provides that Member States must require the implementation of security measures by law.[456] Moreover, on the international level, the Council of Europe's Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data of 23 September 1980 as well as the OECD Guidelines for the Security of Information Systems of 26 November 1992 contain general principles for safety measures.[457]

2. Prohibitions of Security Measures

a. Privacy Protection

As described above, privacy protection includes protection of users against too far reaching personal registration and personal supervision. Thus the above mentioned supranational actions in the field of privacy protection also include instruments prohibiting certain security measures which constitute excessive supervision, e.g., of employers or users of telecommunication services. Since the international initiatives in the field of privacy protection do not contain sector specific prohibitions of security measures so far, reference can be made to the general initiatives mentioned above.

b. Prohibitions of Cryptography

Cryptography issues are relevant for the European Commission with respect to secure electronic commerce which can be provided by the usage of cryptography, especially digital signatures. At this point the INFOSEC-program and especially the Communications from the Commission "A

456 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, OJ L 281/31 of 23.11.1995.

457 See supra IV.A.1.

European Initiative in Electronic Commerce"[458] and "Ensuring Security and Trust in Electronic Communication".[459] have to be mentioned. Especially these two Communications emphasise the necessity of secure cryptographic methods in view of the protection of privacy as well as the use of digital signatures, thus objecting to restrict or even completely ban the use of cryptography.

Furthermore, the OECD Recommendation of the Council concerning guidelines for cryptography policy of 27 March 1997 is of central importance for the future use of cryptography. On the one hand, the significance of cryptography with regard to the development of electronic commerce is emphasised, on the other hand the need of public authorities to have access to data which are not encoded is acknowledged. No preference is given to a specific systems, e.g. "key recovery", and the exact organisation of such a system is left up to the national governments.[460]

The same basic statement is also contained in the "Bonn Ministerial Declaration" adopted on the European Ministerial Conference held in Bonn from 6 to 8 July 1997: In their Declaration, the Ministers acknowledge that the public desire to be granted by law access to encoded data is in principle legitimate as long as the principle of proportionality and the protection of privacy are observed and the measures are efficient.[461]

c. Export Controls on Cryptography

In the European Union, the export of cryptographic software and hardware is restricted by the Council Regulation (EC) No. 3381/94 of 19 December 1994 on the export of dual-use goods, which is in force in all Member States since 1 July 1995.[462] According to its Article 19, this

458 COM(97) 157; cf. <http://www.cordis.lu/esprit/src/ecomcom.htm> (accessed on 24 January 1998).

459 COM(97) 503; cf. <http://www.ispo.cec.be/eif/policy/97503toc.html> (accessed on 24 January 1998).

460 Cf. <http://www.oecd.org/dsti/sti/it/secur/prod/e-crypto.htm> (accessed on 23 November 1997).

461 Cf. <http://www2.echo.lu/bonn/conference.html> (accessed on 24 January 1998).

462 Cf. Council Regulation (EC) No. 3381/94 of 19 December 1994 on setting up a Community regime for the control of export of dual-use goods, OJ L 367/1 of 31.12.1994; amended by Council Regulation (EC) No. 837/95 of 10 April 1995, OJ L 90/1 of 21.04.1995; as well as Council Decision 94/942/CFSP of 19 December 1994 adopted by the Council on the basis of Article J.3 of the Treaty on European Union concerning the control of exports of dual-use goods, OJ L 367/8 of 31.12.1994; as last amended by Decision 96/613/CFSP, OJ L 278 of 30.10.1996 and Council Decision 97/419/CFSP of 26 June 1997, OJ L 178, of 07.07.1997; cf. as well *Kuner*, Rechtliche Aspekte der Datenverschlüsselung im Internet, (1995) Neue Juristische Wochenschrift – Computerreport, pp. 413 et seq. at p. 414.

Regulation limits not only the export of encryption technology to non-EU countries, but also restricts the export among Member States of the EU. Contrary to this, e.g. so-called "public-domain software" is not included in the scope of the Regulation and can be exported freely without any obligations or restrictions.

Moreover, further export limitations for encryption technology result from the Wassenaar Arrangement on export controls for conventional arms and dual-use goods of July 1996. This is an agreement among the representatives of Australia, Austria, Belgium, Canada, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Luxembourg, the Netherlands, New Zealand, Norway, Poland, Portugal, the Russian Federation, the Slovak Republic, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States of America. It covers "dual-use goods" which also includes cryptographic software and hardware.[463]

3. Usage of Digital Signatures

Digital signatures ensure that information sent through open computer networks is examined in so far as to whether the information has been changed during its transportation and to who might be the author of the specified data. Especially with regard to electronic trade among the Member States, the EC Commission has recognised that it is particularly important to find harmonised solutions with respect to the use and the legally binding character of digital signatures or at least to develop harmonised procedures allowing the mutual recognition of digital signatures. Of crucial importance is the need for mutual recognition of the certificates issued by the certification authorities in the individual Member States. A way has to be found by which a certificate issued e.g. by a certification authority in Germany is recognised in France. In its Communication "Ensuring security and trust in electronic communications",[464] the Commission explicitly points out these aspects, which also contains references to pilot projects and to studies backed by the Commission.

On the international level, the UNCITRAL Model Law on Electronic Commerce of 1996 suggests in Article 7 that the legal requirement of a signature of a person is met in relation to a data message if a method is

463 Cf. <http://jya.com/wassenr3.htm> (accessed on 5 January 1998).

464 COM(97) 503 of 8 October 1997. See <http://www.ispo.cec.be/eif/policy/97503.html> (accessed on 24 January 1998).

used to identify the author of a document and to confirm that the author approved the content of that document.[465] Parallel to this, the Working Group on Electronic Commerce of the United Nations' Commission on International Trade Law had the issues of digital signatures and certification authorities on its agenda because the Working Group was requested by the aforementioned Commission to prepare uniform rules on those issues.[466] Recently the Working Group published its Draft Uniform Rules on Digital Signatures, other Electronic Signatures, Certification Authorities and Related Legal Issues,[467] which were also on the agenda of the thirty-second session of the United Nations' Commission on International Trade Law in Vienna during the 19-30 January 1998.[468] In addition to this, the international Chamber of Commerce dealt with the use of digital signatures in electronic commerce in 1997.[469]

G. Conclusions

International and supranational organisations have realised the need for harmonised solutions to fight computer crime at an early stage. They have already considerably contributed to harmonise computer-related law. The main players in this field until now have been the OECD, the Council of Europe and the European Union. Important contributions also came from the P8, the UN, Interpol, and the Association International de Droit Pénal. In the special field of intellectual property protection WIPO and WTO are playing a dominant role.

However, despite these efforts in many areas convincing international solutions are still missing. This is especially the case with the respect to the procedural law problems of computer crime, illegal and harmful contents as well as protection of privacy by criminal law. Most of the existing instruments in these areas are for too vague. The number of international and supranational solutions started in the last two years cannot substitute

---

465 See <http://www.un.or.at/uncitral/texts/electcom/ml-ec.htm> (accessed on 24 January 1998).

466 See <http://www.un.or.at/uncitral/sessions/wg_ec/wp-71.htm> and <http://www.un.or.at/uncitral/sessions/unc/unc-30/acn9-437.htm> (both accessed on 25 January 1998).

467 Cf. <http://www.un.or.at/uncitral/sessions/wg_ec/wp-73.htm> plus the note by the United Kingdom <http://www.un.or.at/uncitral/sessions/wg_ec/wp-74.htm> (both accessed on 27 January 1998).

468 Cf. <http://www.un.or.at/uncitral/sessions/wg_ec/wp-72.htm> (accessed on 27 January 1998).

469 Cf. the study "General Usage for International Digitally Ensured Commerce" <http://www.iccwbo.org/guidec2.htm> (accessed on 24 January 1998).

comprehensive and concrete solutions. On the contrary, especially with respect to illegal and harmful contents al well as procedural law problems today there is a lack of co-ordination among the various organisations who risk starting redundant programs.

In the following, this report will suggest some priority issues for international and supranational organisations. However, before turning to these proposals it is first essential to consider some basic requirements for finding comprehensive solutions to the new challenges of international computer crime.

V. Finding Comprehensive Solutions

The analysis above about computer crime and computer-related criminal law has illustrated a complex pattern of crime as well as a multitude of different new legal problems, which until now are solved in practice independently from each other and without a solid basic concept. As a prerequisite for finding solutions it is therefore necessary to first analyse the fundamental changes of paradigms underlying these new developments (infra A). Based on these findings it is then possible to draw up a comprehensive inventory of the different solutions for preventing computer crime (infra B) before suggesting some priority actions for the European Union (infra C).

A. The Basis of Future Solutions: Analysing the Underlying Shifts of Paradigms

The multitude of new problems of computer crime and computer-related law described above can be traced back to three fundamental changes of today's society: the development from the industrial to the information society and the resulting information law (infra 1), the developing risk society and the resulting importance of non-legal measures for fighting crime (infra 2), as well as the loss of importance of national borders and the resulting need for an international harmonisation of law (infra 3). The analysis of these changes brings to light the key factors for the future dealing with computer crime.

1. Information Society and Information Law

a. Social Changes

The most important power underlying the illustrated changes analysed above is the present development from the industrial to the information society. This development has rightly been called a "second industrial revolution" by economists and sociologists. While the characteristic of the first industrial revolution during the 19th and 20th century was the replacement of manpower by machines, the characteristic of this second phase of industrial development consists in the shifting of human intellectual

activity to machines. This comparison illustrates that the economic and social effects of this new development can surpass the changes caused by the first industrial revolution by far.

This development towards an information society is especially characterised by the fact that beside material objects, immaterial assets like, e.g., deposit money, copyrights, business secrets and other forms of know-how increasingly gain importance. However, information has not only become a new value, but a factor of power with potential dangers. The new risks require special attention and special solutions.

b. Consequences in the Legal System

The analysis of the existing reform laws has shown that this social change of paradigms[470] – from material to immaterial values – has already reached the law. However, a general theory referring to the protection of information is still missing.[471] For this reason, the theory of "information law" or "law of information technology" by the author[472] outlines a general theory concerning the legal status of information and takes these changes into account. In accordance with the findings of cybernetics and computer science, this theory evaluates information as a third basic element next to matter and energy:[473] Information is a new economic, cultural, and political good, but it also creates a special potential danger. The new theory of "law of information technology" realises that modern information technology increases the significance of information: Information becomes an active factor which causes changes in automatic data processing systems without any human involvement; systems of information technology replace human decisions.

This new aspect of "(criminal) information law" shows in particular that the legal assessment of material and immaterial goods must be different.

– A first aspect of the new "information law" deals with the protection of the "proprietor" or "possessor" of material or immaterial goods. In contrast to corporeal objects which, as a rule, are exclusively assigned to

---

470 Cf. for the term "Change of Paradigms" in science *Kuhn*, The structure of Scientific Revolutions, 1962.

471 The respective rules are often developed in analogy to the protection of material objects without sufficiently taking into account the particularities of immaterial goods.

472 Cf. *Sieber*, Informationsrecht und Recht der Informationstechnik, (1989) Neue Juristische Wochenschrift, pp. 2569 et seq.

473 Cf. *N. Wiener*, quoted after *Steinbuch*, (1987) Gewerblicher Rechtsschutz und Urheberrecht, pp. 579 et seq. (at p. 581): "Information is information, not matter or energy. Any materialism which does not admit this can survive at the present day".

certain persons, information is rather a "public good" which, in an open society, must flow freely and must therefore not be protected by rights that exclude all others. These basic principles of "freedom of information" and "unrestrained flow of information" are an essential prerequisite for a free economic and political system.[474]

- A second particularity of the legal assessment of immaterial goods follows from the fact that protection of information must not only take into account the economic interests of the proprietor, but at the same time also the interests of those who are concerned by the content of the information. The new requirements for the protection of privacy in the field of electronic data processing resulted from this aspect of information which does not exist with regard to material objects.
- A third difference between information and corporeal goods is the fact that information can be transferred and copied easily and anonymously. Therefore, it is often difficult to trace back the author of information. As a consequence the question gains special importance in how far intermediaries transporting or storing third party information (such as service providers) can be held responsible for this content.
- With the increasing importance of information, the rights giving access to information gain significance – not only for criminal prosecution authorities but also (e.g. in data protection law) for any citizen (so-called "access to information rights").[475]

Thus, it becomes obvious that legal rules for information cannot be developed by way of analogy from provisions on corporeal objects, but that they need their own independent basis and theory. For criminal information law, the consequences of this general theory are evident: A limited protection of the creator of information, the protection of the citizen concerned by information, the protection against illegal and harmful contents of information as well as the access to information are also to be guaranteed by criminal law – in so far as other measures are not sufficient. "Intellectual property", "privacy", "absence of illegal and/or harmful contents" as well as "access to information rights" describe the new objects

474 Cf. *John Stuart Mill*, On Liberty, 1859; *Popper*, The Open Society and Its Enemies, 2nd ed., 1945.

475 Cf. for the access to information rights in the different countries the articles in Sieber (ed.), Information Technology Crime, 1994, especially for Brazil *de Araujo Jr.* (pp. 82 et seq.), for Canada *Piragoff* (p. 120), for Germany *Möhrenschlager* (p. 212), for Hungary *Kertész/Pusztai* (p. 253), for Italy *Lanzi* (p. 301), for Luxembourg *Jaeger* (p. 332), for the Netherlands *Kaspersen* (p. 359), for Romania *Antoniu* (p. 416), for Spain *Gutiérrez Francés* (p. 439), for Tunisia *Ben Halima* (p. 477), and for Turkey *Erman* (pp. 484 et seq.). Cf. for the German legal situation *Lodde*, Die Informationsrechte des Bürgers gegen den Staat, 1995.

of legal protection, which have not only provided the basis for the previous reform legislation, but which can, in the information society at the verge of the 21st century, rightly claim protection by criminal law as well. This explains why so many new legal questions have to be dealt with in the information society.

2. Risk Society and Changed Risk Control

a. General Social Changes

The increasing significance of information in the post-industrial information society described above is mainly caused by the development and expansion of information technology. The development of the technological society and of technology law is, therefore, the second major force of change behind the singular questions analysed above. Since the 1980s, sociologists and lawyers have been discussing the social impact of modern technology under the term of "risk society".[476] A presentation of this academic discussion must, therefore, necessarily precede an analysis of how far the ascertained changes of general technology are valid also in the field of information technology.

Since the 1980s, the discussion about the risk society in Western countries focused on the general technology dangers of chemistry, nuclear energy, genetic engineering and of other installations with possible harmful impacts on man and nature. The actual changes dealt with in the discussion can be traced back to three main aspects:

- New risks with greater impact arise which cannot be limited in space, time or with regard to the group of persons affected.
- In many fields,[477] risks have acquired a "social dimension" and cannot be traced back to individually responsible persons.
- The complexity and the speed of development of social and technological changes are increasing.[478]

476 I.e. the "epoch in which the dark sides of progress more and more rule social conflicts". Cf. Beck (ed.), Politik in der Risikogesellschaft, 1991, p. 10, as well as the basic work of *Beck*, Risikogesellschaft, Auf dem Weg in eine andere Moderne, 1986. For the meaning of this term for criminal law cf. *Prittwitz*, Strafrecht und Risiko, 1993.

477 For example the hole in the ozone layer, water pollution or floods.

478 Cf. *Stratenwerth*, 105 (1993) Zeitschrift für die gesamte Strafrechtswissenschaft, p. 681.

b. General Consequences in the Legal System

The resulting legal changes – until now especially discussed in environmental law – can be reduced to three lines of development as well:

- With respect to greater risks, an improved crime prevention by social politics, but also a more powerful state and intensified legal control are called for by many persons. However, even with intensive state interventions using criminal law, the new risks can no longer be controlled by repressive criminal law measures only. Instead, the repressive approach of criminal law must be amended by preventive regulations.[479] Since criminal law does no longer suffice to control the new risks, alternative (e.g. technical, economic or structural) solutions become more and more important.
- The social dimension of risks leads to risk communities, solutions by insurance law, new objects of legal protection and strict liability. It is especially controversial in how far criminal law can solve the problems mentioned. On the one hand, wider rules of imputation and protective concepts are called for, on the other hand, a reduction of criminal law is demanded as it is regarded inappropriate for the regulation of social dimension risks and for a risk balance independent of fault because of its classic needs for imputation.[480]
- Because of the greater complexity and dynamism, the law makes more and more use of indefinite legal terms, of blanket clauses and dynamic references. Rule-making by private organisations (especially so-called

---

479 Cf. *Albrecht*, (1988) Kritische Vierteljahresschrift, p. 182 (at p. 209); *Callies*, (1989) Neue Juristische Wochenschrift, pp. 1338 et seq.; *Hassemer*, (1989) Neue Zeitschrift für Strafrecht, p. 553 (at p. 558); *Hilgendorf*, (1993) Neue Zeitschrift für Strafrecht, p. 10 (at pp. 13 et seq.); *Kuhlen*, (1994) Goltdammer's Archiv für Strafrecht, pp. 347 et seq.; *Wolf*, 15 (1987) Leviathan, pp. 357 et seq.

480 Cf. for the first opinion *Stratenwerth*, 105 (1993) Zeitschrift für die gesamte Strafrechtswissenschaft, p. 679 (at pp. 691 et seq., 659); *Tiedemann/Kindhäuser*, (1988) Neue Zeitschrift für Strafrecht, p. 337 (at pp. 339 et seq.); for the opposite opinion cf. *Calliess*, (1989) Neue Juristische Wochenschrift, pp. 1338 et seq. (at p. 1343); *Hassemer*, (1989) Neue Zeitschrift für Strafrecht, p. 553 (at p. 558). Analysing these questions with respect to computer-related crime one can say that the development of crime and law in the field of information technology disproves of this particular sector the global, general criticism of a too far-reaching "risk criminal law". The new criminal provisions and likewise the new procedural powers of intervention for criminal investigations in the field of information technology are predominantly justified by the social changes presented. Legal policy must nevertheless accept the reproach that non-criminal measures have been neglected and that a partly insufficient legal technique has been used.

self-regulation) increases.[481] Apart from this, the correlation between different fields of law becomes closer; new intermediate fields emerge.[482]

c. Information Technology as Part of the Risk Society

The analysis in this report has demonstrated that most of the changes described above of the risk society also occur in the field of information technology: Small alterations of data can move large amounts of deposit money. Computer sabotage – for example in banks or with flight control systems – affects the most vital parts of the modern economy. Complexity and speed of development are growing. Accordingly a lot of the general findings and controversies concerning the "law of the risk society" apply to the field of information technology as well:

- The future information society requires mainly non-criminal measures for the prevention of computer crime. Technical security standards that include access control systems, instructions for the system users concerned, awareness and education programs as well as appropriate general conditions of civil and administrative law in many cases are more important than criminal law provisions.[483]
- However, at the same time an adaptation of criminal law to the new risks is necessary: The general reproach of an over-criminalisation by the protection of collective interests as well as the use of "per se bans" and strict-liability offences of "risk criminal law"[484] is not justified in this analysed field of information technology.[485] In the emerging risk society,

---

481 Cf. for the regulatory techniques in the field of environmental law *Hoppe/Beckmann*, Umweltrecht, 1989, pp. 41 et seq., 159. For the constitutional problems of these regulatory techniques cf. *Denninger*, Verfassungsrechtliche Anforderungen an die Normsetzung im Umwelt- und Technikrecht, 1990, pp. 31 et seq., 79 et seq., 117 et seq., 148 et seq. For the problems concerning the participation of expert committees in legislation cf. *Hofmann*, Privatwirtschaft und Staatskontrolle bei der Energieversorgung durch Atomkraft, 1989, pp. 42 et seq.

482 A popular example for such an intermediate field is – besides information law – especially environmental law.

483 Cf. for the necessity of a stronger political (non-legal) control of technological and economic sectors from the discussion about the risk society especially *Albrecht*, (1988) Kritische Vierteljahresschrift, pp. 182, 205, 209. In particular on computer crime cf. *Sieber*, The International Handbook on Computer Crime, 1986, pp. 117 et seq.; cf. especially for organised crime *Sieber/Bögel*, Logistik der Organisierten Kriminalität, 1993, pp. 287 et seq.

484 Cf. especially *Hassemer*, (1989) Neue Zeitschrift für Strafrecht, pp. 557 et seq.; *Hassemer*, (1992) Zeitschrift für Rechtspolitik, pp. 378 et seq.

485 The presented analysis of "information law" has shown that improved criminal law protection in the field of intangibles – especially with respect to intellectual property and the citizen's right to privacy – is justified by new needs for protection in the information society. Problems of imputation concerning the risk society as well as the resulting "per se bans" can hardly be noticed in the field of criminal information law. Only in the field of criminal data protection law is there an

the new values and objects of the information society need criminal protection.

- Legal regulations must not concentrate on coincidental technological changes as was done in many national legislations. What is necessary is structural thinking and a description of the functions thus resulting to law which can also deal with changing technology.[486]

3. Global Society and International Legal Harmonisation

a. Social Changes

The third general line of development behind the problems described here is the loss of importance of national borders and the corresponding international harmonisation of law. The coming together of the citizens of the world – in general related to a greater mobility – can be seen in the field of computer crime particularly with the use of international telecommunication networks: The mobility of data in these networks makes it possible to commit a crime with the help of a computer of which the results take place abroad. Data can be transferred via international networks in a split second without having any possibilities of control. These changes entail a loss of power of the traditional national state both in favour of regional and supranational governmental organisations as well as in favour of multinational companies, but also with respect to organised crime groups.[487]

b. Consequences in the Legal System

Therefore, the effective protection of the citizen in the newly emerging information and communication society is only possible if these basic changes are considered and shaped positively. Global approaches are necessary to have an intensified co-operation of national states and supranational organisations, both with respect to legal measures and in developing new comprehensive and prevention strategies.

Different national laws with the aim of preventing computer crime would entrain "data havens" or "computer crime havens" which, in turn, would

---

over-criminalisation, which is however not due to the creation of new collective objects of legal protection or "per se bans", but to disregarding the classic ultima-ratio principle of criminal law.

486 Cf. *Sieber*, Informationstechnologie und Strafrechtsreform, 1985, pp. 33 et seq.

487 For a more detailed analysis of these aspects see memorandum of *Sieber*, A Model European Penal Code, Council of Europe, AS/Jur (1996) 76 of 5 February 1997.

lead to market restrictions and national barriers to the free flow of information. These restrictions and national barriers would not only be established by companies which would cease to export computer programs into those countries that do not have an effective legal system of protection for computer software. Different legal regimes would also provoke governments to restrict data flows to countries with less developed protective systems, as is illustrated by export regulations for personal data in many privacy laws. These national restrictions (such as access control with respect to illegal contents) would imperil privacy, trade secrets and the free economic development of an international information market. Different preventive measures could also affect equal conditions of competition.

Above all, national solutions and restrictions for the free flow of information would be doomed to failure. This is illustrated especially by international telecommunication networks in which data can be transferred in an encoded form by a telephone call with a duration of only a few seconds. Considering the amount of both private and public data transferred in international computer networks controls of their content are no longer possible. Similarly, it is impossible to control corporeal tapes, discs, compact discs and computer chips which are transferred from one country to another. The political liberalisation in Central and Eastern European countries, which was supported considerably by the transfer of Western information, made obvious that information is free and can hardly be controlled by governments.[488]

In addition, with respect to procedural law, the harmonisation of the various national coercive powers is an important factor for the smooth functioning of the international instruments of mutual assistance, since – even if the requirements of double criminality are fulfilled – a state whose assistance is requested can only carry out measures admissible by its law. In the long run, in close cultural and economic communities such as in Europe, a harmonisation of coercive powers and the respective legal safeguards could make specific and complicated routines of mutual assistance obsolete and give the decision of a future "European" or internationally recognised judge the same value as the decision of a national authority.[489]

---

488 Globally used rating systems could change this result only in a very limited way since they can only be used in specific sectors of data flows (e.g. not covering private or dynamic or short-living data exchanges).

489 See *Sieber*, Procedural Law Problems with Regard to the Use of Computerized Data in Criminal Investigations, Council of Europe, Report No. PC-R-CC-89-3 of 23 February 1989; *Sieber*, Internationale Erforschung und Bekämpfung der Wirtschaftskriminalität, in: Albrecht/Sieber (eds.),

B. Remedies to Fight Computer Crime – A General Approach

The analysis of paradigms shifts behind the multitude of new cases and new laws make it obvious that fighting computer crime can no longer focus on amending traditional national criminal law as it is still considered by politicians in many countries: Instead, the following three main findings of the above analysis have especially be taken into account:

- In the modern risk society the main efforts to reduce risks must focus on technical, structural and educational measures.
- In the global society – especially in international communication networks – all technical or legal efforts must be international.
- In the information society new (especially legal) approaches must consider the specifics of information as a new value but also as a new risk potential.

Consequently, the problems of computer crime can only be solved by a combination of concerted international actions. These actions should comprise especially the following four "filters" to fight crime: Technological and organisational measures, education, industry and the law.[490]

1. Technological and Organisational Measures

Computer crime problems are mostly technical and/or organisational problems of the victims of computer crime. As a consequence technical and organisational solutions are the most important means to prevent computer crime. These measures include personal and educational safety, physical safety, organisational and technical safety, internal auditing, insurance against computer crime as well as the proper formulation of contracts. The majority of these measures must not only be restricted to the prevention of computer crime, but should also aim at threats caused by negligence,

Zwanzig Jahre Südwestdeutsche Kriminologische Kolloquien, 1984, pp. 29 et seq., at 51 et seq., 57 et seq.; *Sieber*, Europäische Einigung und Europäisches Strafrecht, 103 (1991) Zeitschrift für die gesamte Strafrechtswissenschaft, pp. 957 et. seq.

490 This combination of measures to fight computer crime has been developed in the expert group of the G8 Ministers and Chief Advisors of Science and Technology (Carnegie-Group). See supra chapter IV.D.2, fn. 438.

human errors, professional incompetence, natural occurrences and environmental forces, as well as labour strikes.

Following the Recommendation of the above mentioned expert group of the P8 Ministers and advisors of science and technology on "Misuse of International Data Networks"[491] technical solutions should especially promote the development and use of

- technologies that will authenticate the user to the service and, conversely, authenticate the service to the user,
- technologies that can enhance security of communications through each link of the communications chain from the individual (personal or company) user device all through the network (e.g. by minimum security standards and security "audits"),
- appropriate non-repudiation services, e.g., providing secure digital signatures by secure user devices, asymmetric crypto systems and certified public keys,
- technologies for tracking Internet communications or in other cases, quite the reverse for the use in other cases, anti-monitoring systems, i.e., anti-tracking technology, to protect the privacy of users by preventing unnecessary gathering and linking of data,
- measures against the abuse of anonymity, e.g., non-repudiation services based on certified pseudonyms where the certification authority is able and obliged to furnish the name and address of the holder of the pseudonym under clearly defined circumstances,
- international frameworks to enable the use of effective encryption world-wide,
- technologies for effective monetary transactions (especially anonymous digital cash) which are necessary for commerce in the Internet and which have to be secure and protect the privacy of users on the one hand, but – on the other hand – have provisions to discourage their use for criminal purposes (e.g. money laundering),
- technologies for content rating, e.g. voluntary labelling and filtering technologies (e.g. PICS), including self-rating for web sites and news group articles,
- technologies for copyright protection, i.e. watermarking and authentication technologies as well as a time stamping service to protect intellectual property.

491 See supra chapter IV.D.2, fn. 438.

2. Awareness and Education

In most of the above described illegal actions, computer crime was enabled by the fact that computer users did not apply existing technical protection measures. E.g. poor designs of security features, negligence with respect to passwords or missing back-up systems can be frequently found. As a consequence it is most important to raise public awareness on the vulnerability of computers and communication systems and on the respective security features. This can be done e.g. by education in schools and universities, general awareness campaigns, seminars, independent security consultants, hard- and software manufactures, online service and access providers, insurance companies, research institutes, intelligence services and other governmental agencies.[492]

However, the role of education goes far beyond raising awareness of risks and teaching security procedures. It should aim at broad multimedia competences. Following the Recommendations of the expert group of the P8 Ministers and advisors of science and technology[493] mentioned above education should

- advise political leaders on any new areas where new policies may be appropriate with respect to the prevention of misuse in data networks,
- raise public awareness of the Internet as a valuable tool for education and lifelong learning, as well as of the importance of promoting the responsible use of this new medium,
- develop increased access to computer networks, services and contents for schools and universities,
- create a favourable environment for easy use of the Internet for everybody, especially the younger generation, e.g. by linking or creating "electronic townhalls", where students from participating nations can share views and experience regarding the Internet,
- educate users on their rights, duties, and procedures for safe use of the Internet, for example by:

  promoting the use of filtering software,

492 Examples for the improvement of data security by governmental assistance are the foundation of the Dutch "Platform Computercriminalität" in 1989 (a project of the Dutch Ministries of Justice and Commerce in co-operation with private organisations of commerce and industry) or of the German "Bundesamt für Sicherheit in der Informationstechnik" in 1990 (an agency under the German Ministry of Interior Affairs) in order to improve data security in the private and the governmental sector.

493 See supra chapter IV.D.2, fn. 438.

informing users of regulations/laws concerning data protection, intellectual property rights and related criminal laws,

providing information to help users select secure personal devices and communication systems and on procedures for the use of anonymity,

- educate users on how to be well-informed consumers of new electronic commerce services, for example the collection of transactional records needed to resolve disputes,
- provide educators with learning opportunities on the use and potential danger of international data networks.

3. Information and Communication Industry

Besides users, the education system and governments, it is especially the information and communication industry that plays a key role in fighting computer crime. The computer and communication industry can be decisive in developing technical solutions, creating a safe infrastructure, and educating users. Considering the global aspects of computer crime, the industry is a key player especially since it is acting internationally and is not bound to national borders as is the case with governments. Following the Recommendations of the above mentioned expert group of the P8 Ministers and advisors of science and technology,[494] voluntary measures of industry could therefore

- improve security and the usability of security mechanisms,
- advise users and providers on how to use security technologies and procedures,
- undertake work with governments on educational issues,
- establish codes of conduct, thereby setting an international industrial norm for illegal contents and illegal actions as well as reasonable action against illegal content/action,
- consider methods to promote accurate voluntary labelling and the development of "acceptable use policies", while the use of labelling for (private) censorship or discrimination against competitors has to be prevented,
- create an international network of contact points which can react in cases of illegal contents, once made aware of them,

494 See supra chapter IV.D.2, fn. 438.

- specify actions when alerted to the existence of illegal material or activity, thereby limiting service providers' liability under the law,
- define protocols for working with law-enforcement agencies,
- foster electronic commerce and the free flow of information by developing policies on anonymous digital cash and anonymous electronic transactions that protect public safety without hindering technological progress,
- foster the development of trusted third parties (for authentication, identification, and prevention of fraud).

4. Legal Measures

Legal measures play a dominant role in order to prevent specific illegal activities by educating and deterring users, sanctioning perpetrators and compensating victims. However, legal measures must not be restricted to criminal law but should also include civil and administrative regulations (e.g. with respect to civil liability of providers, prescription of minimum protection standards by administrative law in areas where third party interests are concerned). In the field of criminal law they should not only cover adequate substantive law regulations but also enable effective prosecution, however at the same time being adequate safeguards for the human rights of suspects and witnesses as laid down in the European Convention of Human Rights and Fundamental Freedoms. Due to the international dimensions of computer crime they should be co-ordinated, harmonised or unified on a international or supranational level. The aforementioned expert group of the P8 Ministers and advisors of science and technology on "Misuse of International Data Networks"[495] has stressed especially measures to:

- strengthen international mechanisms for addressing illegal actions, e.g. by creating a well-defined set of international minimum rules against illegal actions, such as hacking (illegal access to and penetration of information systems), computer espionage, computer sabotage, computer fraud and copyright infringements,
- strengthen international mechanisms for addressing illegal contents, e.g. by creating a well-defined set of international minimum rules for illegal contents to be prosecuted and punished world-wide, especially with respect to child pornography, bestiality, the glorification of violence, hate speech as well as defamation of minorities and individual persons,

495 See supra chapter IV.D.2, fn. 438.

- encourage countries to define an adequate system of rules for the responsibility of Internet access providers and service providers, e.g. by creating a legal system so that in all countries service providers must undertake reasonable efforts to erase illegal contents on their servers when made aware of these contents, while at the same time the free flow of data should not be hindered by – generally unsuccessful – attempts to block access to other servers and by holding access providers liable,
- encourage countries to establish national laws for the effective prosecution of computer crimes, especially with respect to search and seizure of computer systems and international networks, duties of witnesses (e.g., to provide passwords or to decrypt files), wiretapping and accessing computer systems,
- address possible abuses of anonymity, and install an international system for lifting anonymity in cases of abuse, thereby requiring adequate legal safeguards for privacy rights (e.g. by demanding court orders as a prerequisite for transferring specific data to the prosecuting authorities), thereby considering the fact that lifting anonymity is only possible, if all countries co-operate, which are crossed by the communication (because as long as there are countries which do not co-operate, anybody wishing to hinder the lifting of his/her anonymity, merely has to provide for routing through one of these countries),
- develop an international information network and other information systems with respect to the prosecution of illegal and harmful practices detected on the Internet,
- foster co-operation among law enforcement agencies, with special respect to urgent measures for "freezing" data in international search and seizure procedures,
- clarify issues of jurisdiction,
- educate and train law enforcement agencies about cyber crime and its prosecution.

C. Priority Actions for the European Union – Focusing on Non-Legal Measures

Due to the international character of computer networks all of the above dealt with remedies require European and international co-ordination. As a consequence it could be useful, if the European Union would support – within the range of its competence and with special respect to the subsidiarity – the development and co-ordination of all these actions.

However, since the means of the European Union are limited and since the duplication of work done by other international organisations should be avoided, the European Union must select some priority actions.

Taking into account the work already accomplished or undertaken by other international bodies the present report suggests the following (especially non-legal)[496] priority actions which could be developed by the Commission and/or the Council:

1. Studying the Links of High Tech Crime and Organised Crime

The above analysis showed that there are special features (such as anonymity, encryption, or international flexibility) that make the use of computer technology and computer crime attractive for criminals, especially for organised crime. These "criminogenic" factors of computer technology and the links between high tech crime and organised crime should be studied in more detail with the aim to avoid crime incentives and technological developments which later could be irreversible and support the commitment of crime. Considering the above mentioned "Action Plan to Combat Organised Crime"[497] this study should be initiated by the Council. It could be based on the findings of the present report and the work of the P8 subgroup on High-Tech Crime. The study could start with a questionnaire to be sent to the Member States, some non-Member States with special experience in fighting high-tech crime (as the United States of America and Canada) and to competent international bodies (such as P8, Interpol and Council of Europe). Drafting the questionnaire in a professional manner will be the key issue for the success of a later study and for practical recommendations.

2. Awareness and Education

The present study illustrated that users, industry, governments, lawmakers and politicians are not sufficiently aware of the vulnerability of the information society, the threats of computer crime and the possible protective measures. As a consequence, raising awareness and education is a major instrument to reduce the risks of computer crime. The Commission

496 The proposed legal measures of the EU are developed infra chapter VI after the analysis of the respective competences of the EU.

497 See supra chapter IV.E.2.e, fn. 451.

and the Council should support this process, e.g. by the publication of communications and green books, material for teaching students and users (e.g. by new multi media products on CD-ROM) and other information campaigns.

3. Development of Technology and Emergency Response Teams

The present study explained that the most effective means against illegal actions in the field of computer crime are technical and organisational safety measures. In co-operation with industry and governments, the Commission should therefore foster the development of technological safety measures and emergency response teams in order to protect users. Since the technological problems are the same in all countries this development could be supported and co-ordinated on an international level. Awareness campaigns on computer crime and joint international research projects should give incentives to develop not only effective but also safe products. Considering the threats of computer crime to electronic commerce special emphasis should be put on the development of effective monetary transactions. These transactions should be safe, guarantee the privacy rights of the users but at the same time permit an effective money laundering control and criminal prosecution.

4. Creating a Network of Contact Points for Illegal Contents

The above analysis demonstrated that illegal contents can not be controlled by creating national barriers against specific data since this is neither technically possible nor socially desirable (as it would hinder the international free flow of data and lead to an Orwellian supervisory system). Illegal and harmful contents must – instead of being blocked in transition – be removed from their servers. In order to enable fast and global removal of illegal and harmful contents an international network of contact points is necessary which can disseminate information on such contents to the operator of the relevant servers (which, when made aware of illegal contents should have a legal duty to remove the respective data).

Following the above mentioned "Action Plan on Promoting Safe Use of the Internet",[498] the Commission and the Council should support the

498 See supra chapter IV.D.1.b.

establishment of such contact points which can be run either by the governmental sector or – as self-regulative bodies of industry – by the private sector.

5. Supporting International Industry Codes of Conduct

The legal analysis of this study demonstrated that the harmonisation of legal rules in general is a slow process. On the other side multi-national and globally operating companies often have less difficulties to arrive at international solutions. As a consequence, industry should try to develop informal rules (soft law), such as codes of conduct. These rules could set up minimum standards for illegal contents and for privacy protection of users as well as protocols for co-operation with the criminal law prosecution system in accordance with national law (e.g. asking to lift the anonymity of perpetrators). Such industry codes of conduct and other forms of soft law could also successfully influence the later harmonisation of hard law. The Commission should support the development of these codes of conduct by bringing together the relevant players of the industry and giving them the necessary floor as well as by providing a favourable legal environment to develop these rules (e.g. by considering codes of conduct in the legal responsibility regimes).

6. Development of Trace Back Procedures

The study showed that one of the main problems for prosecuting computer crime is the anonymity provided by international computer networks. This anonymity must not be completely removed since privacy protection for users and anonymity (e.g. for social minority groups) is an important social value which should not be given up in international computer networks. However, on the other side, it should be possible, under well-defined legal circumstances (such as court orders) to lift anonymity in order to trace back the authors of illegal actions (such as hackers) or of illegal or harmful contents (such as paedophiles). Today such trace back procedures are often hindered or made impossible due to the features of the TCP/IP protocol of the Internet and in addition especially by the activities of anonymous remailers and the use of free access software.[499]

499 See supra II.C.

With respect to an effective prosecution of computer crime it is therefore most important to set up a working group of technical and legal experts in order to study existing trace back procedures and ways to improve them. Since this will include necessary changes of the TCP/IP protocol it is most important that the respective industry is co-operating and represented in this project. Co-operation of representatives from the prosecution system is also most important to define their needs. On the other hand representatives of privacy protection should also be included in the group. The group should take into account the work already done and presently being undertaken by the P8 subgroup on High Tech Crime. The EC should support the P8 subgroup and the establishment of a special working group concentrating on the respective technical questions and/or a study on this most crucial point.

7. Legal Measures

The above legal analysis showed that the prosecution of computer crime is extremely hindered by a major contradiction: On the one hand there are globally operating perpetrators which can freely exchange data in milliseconds all over the globe. On the other hand there are prosecuting agencies which – due to the principle of state sovereignty – are limited to their national territory, an obstacle that can only be overcome by slow, burdensome, bureaucratic and ineffective means of mutual assistance. Such a system cannot work and is doomed to failure.[500]

As a consequence, mutual co-operation, harmonisation of laws as well as supranational and international prosecution systems must be strengthened. However, this does not only raise difficult political questions since criminal law is still perceived as a domain of national sovereignty. With respect to possible actions within the European Union there are also intricate – legal and political – questions of competence. For this reason the respective actions in the legal area first require an analysis of competence which will be dealt with in the following chapter.

500 Cf. *Sieber,* Memorandum for a Model European Penal Code, Council of Europe, AS/Jur (1996) 76 of 5 February 1997 (published in a German translation in 1997, Juristenzeitung, pp. 369 et seq.).

VI. Competences and Priority Actions of the European Union with Respect to Legal Measures

When looking for legal countermeasures of the European Union against the above described forms of computer crime, there are two fundamentally different possible paths that can be used for finding such solutions: The first path is offered by the EC Treaty, which forms the supranational "first pillar" of the European Union. The second possibility lies within the ambit of the so-called "third pillar" of the European Union, i.e. intergovernmental co-operation in Europe in matters of home affairs institutionalised by the K Articles of the Treaty on European Union ("the Maastricht Treaty") in 1993.

Up to now, the fight against crime in the European Union has mainly been carried out in the context of this third pillar, in particular by agreeing on international conventions, e.g. in the field of fraud against the budget of the EC.[501] First pillar initiatives in the field of crime and criminal law have not played a dominant role so far. This has been the case because of legal necessity, but also because of political determination. Nonetheless, a closer look should be taken at the EC's competence to adopt supranational measures against computer crime in the framework of the first pillar, because such directives and regulations have a far more compelling effect on Member States – legally rather than politically – than international treaties agreed upon in the framework of the third pillar. The following section will thus analyse in how far computer crime can be countered by first pillar actions such as regulations or directives (infra A), before a closer look is taken at conventions and joint actions or – after the entry into force of the Amsterdam Treaty – framework decisions in the context of the third pillar (infra B).

501 See, e.g., Convention, drawn up on the basis of Article K.3 of the Treaty on European Union, on the protection of the European Communities' financial interests, OJ C 316/48 of 27.11.1995.

A. Actions Covered by the First Pillar

1. The Distribution of Powers

a. General Principles

In most federal legal systems, the distribution of powers between the central authority and the regional entities often gives rise to legal disputes delineating the respective spheres of action between the players of the federal game. Even though the European Community is not a federal system, the delicate balance of powers and the distribution of competences between the supranational body and the Member States is of central importance in its legal system, too. The European Community was created by the Member States irrevocably conferring sovereign powers to the new supranational entity. From this historic background and from the wording of various Treaty provisions,[502] the fundamental principle is deduced that the EC is only empowered to take actions in those fields that have explicitly been attributed to the Community by the Member States.[503] Moreover, as regards the actual type of measures to be adopted – in particular directives and regulations according to Article 189 of the Treaty – the EC can only enact those measures that are specifically allowed by the legal basis.[504]

Most powers of the EC are non-exclusive ones, meaning that Member States remain competent to legislate also in those fields which have explicitly been attributed to the Community as long as the EC has not taken action in these same fields. In this area of

502 Cf. e.g. Article 3b (1): "...within the limits of the powers conferred upon it by this Treaty..."; Article 189 (1): "...in accordance with the provisions of this Treaty...".

503 The so-called "compétences d'attribution", see ECJ, Case 188-190/80, (1982) ECR, pp. 2545, at p. 2573.

504 This fundamental principle is sided by the doctrine of "implied powers", a principle known both in public international law and in the interior legal order of the Member States, according to which the Community holds, irrespective of the wording of an empowering provision, all the additional competences necessary to effectively fulfil the powers that have explicitly been attributed. The system of distribution of powers is completed by Article 235 of the EC Treaty, on the basis of which the Community can adopt adequate measures for achieving the aims of the EC Treaty if it does not provide for explicit powers. Last but not least, the European Court of Justice has established that the Community holds parallel exterior powers to conclude agreements with international organisations and third countries in all areas in which it holds the interior competence according to the principles stated above (cf. ECJ, Case 22/70, Decision of 31 March 1971, (1971) ECR, p. 263; Legal Opinion 1/94 of 15 November 1994, (1994) ECR, p. I-5267; Legal Opinion 1/92 of 10 April 1992, (1992) ECR, p. I-2821; also cf. Case C-327/91, Decision of 9 August 1994, (1994) ECR, p. I-3641).

"parallel competences",[505] the principle of subsidiarity, introduced by the Maastricht Treaty to Article 3b (2) of the EC Treaty, has the main function to limit the competence of the Community in these areas: It means that despite a given power in a certain field, the Community can only take actions if a certain aim acknowledged in the Treaty cannot be sufficiently achieved on Member State level, and if the aim can be better achieved, with respect to the scope and the effect of a Community measure, on Community level.[506] On the other hand, if an envisaged Community action promises such "added value" as compared to Member States' actions, the Community is then empowered to legislate on the basis of the EC Treaty. In view of the fact that computer crime is often, but not necessarily, of international nature, the principle of subsidiarity thus fulfils an important role in delineating powers between the EC and the Member States for the particular area of parallel competences.

b. EC and Criminal Law: Distinguishing Prohibition and Sanction

The analysis of the legal regimes of numerous countries with regard to computer crime showed that most countries will consider the relevant activities as punishable criminal offences. Therefore, the major question to be answered is whether the EC is empowered, irrespective of the actual legal basis on which measures are adopted, to counter computer crime also with criminal law measures or at least with measures of criminal administrative character. This question is problematic mainly because it is often noted that the EC has no power whatsoever concerning "criminal law".[507] In the present context, however, this statement is far too global and imprecise by nature: It does not distinguish adequately between the prerequisites, i.e. duties to fulfil or to omit, of a criminal norm on the one hand and the sanction contained in a criminal norm on the other hand, let alone between different kinds of sanctions and different ways how sanctions can eventually be put into effect in the Member States.

The distinction between the prohibitory part of a criminal norm on the one hand and the sanction contained in a criminal provision on the other hand is not new, but has a

505 Cf. *Zuleeg*, in: Groeben/Thiesing/Ehlermann (eds.), Kommentar zum EU/EG-Vertrag, Art. 3b, para. 6.

506 See *Beutler/Biber/Pipkorn/Streil*, Die Europäische Union, 1993, p. 85.

507 Cf. the references quoted by *Dannecker*, Strafrecht der Europäischen Gemeinschaft, in: Eser/Huber (eds.), Strafrechtsentwicklung in Europa, 1995, p. 2004, fn. 138 and 139; by *Sieber*, Das strafrechtliche Sanktionensystem zum Schutz der europäischen Gemeinschaftsinteressen, in: van Gerven/Zuleeg (eds.), Sanktionen als Mittel zur Durchsetzung des Gemeinschaftsrechts, p. 71, at p. 77, fn. 29; by *Tiedemann*, Europäisches Gemeinschaftsrecht und Strafrecht, (1993) Neue Juristische Wochenschrift, p. 23, fn. 1, as well as by *Cuerda*, Besitzt die Europäische Gemeinschaft ein ius puniendi?, in: Schünemann/Suárez Gonzalez (eds.), Bausteine des europäischen Wirtschaftsrechts, Madrid-Symposium für Klaus Tiedemann, 1994, p. 367, at 368 (fn. 4 and 5). Also cf. ECJ, Case 203/80, (1981) ECR, p. 2595, at 2618.

long tradition in legal science.[508] This distinction is immanent in each and every traditional criminal norm: E.g., a traditional provision on murder contains the prohibitory part that people shall not kill, and the subsequent sanction that an infraction of the prohibition entails a life imprisonment. As was illustrated above,[509] in the field of supplementary criminal law ("Nebenstrafrecht"), the prohibition is not even specified in a criminal law provision itself, but in civil or administrative provisions, e.g. in copyright law (the prohibition to copy works of an author) or in data protection law (the prohibition to process specified personal data), and the actual criminal law provision only regulates the sanction.

This traditional distinction can be found in a comparable manner in EC law, too: Previous activities of the EC show that the Community has regulated a prohibition or other duties to comply with – which actually constitute the prerequisites of an eventual national criminal norm – by a directive adopted in the framework of economic harmonisation without regulating the corresponding sanction itself in detail:[510] The Insider Dealing Directive,[511] based on Article 100a, requires Member States to prohibit certain activities with respect to insider dealing and also specifies the group of people which have to comply with these duties (Article 2 of the Directive), but the choice of the actual sanction for infractions against these duties is left, at least to a certain degree,[512] up to the Member States' discretion. Likewise, the Money Laundering Directive of 1991[513] explicitly requires Member States to prohibit money laundering as such (Article 2), whereas it only provides that Member States must enact "*adequate measures*" in order to ensure the effective application of all provisions of the Directive (Article 14). This obligation includes, in particular, the duty to lay down rules stating how infractions against the Directive will be sanctioned, but again, the Directive only regulates the prohibition and not the sanction itself. Similarly, the 1995 EC Data Protection Directive[514] dealt with above, regulates the lawfulness of the

508 Cf., e.g., the German criminal lawyer *Binding*, who distinguished "Verbotsnormen" (prohibitory provisions) addressed to the citizens and requiring a certain behaviour, from "Sanktionsnormen" (sanctioning provision), which are addressed to judges and tell them how a certain infraction should be punished.

509 Chapter III.G.

510 Cf. *Tiedemann*, Europäisches Gemeinschaftsrecht und Strafrecht, (1993) Neue Juristische Wochenschrift, pp. 23 et seq, at p. 26.

511 Council Directive 89/592/EEC of 13 November 1989 coordinating regulations on insider dealing, OJ L 334/30 of 18.11.1989.

512 Cf. infra chapter VI.A.3.c.

513 Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering, OJ L 166/77 of 28.06.1991.

514 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, OJ L 281/31 of 23.11.1995.

processing of personal data in detail and provides, in Article 24, that the Member States "shall adopt suitable measures to ensure the full implementation of the provisions of this Directive and shall in particular lay down the *sanctions* to be imposed in case of infringement of the provisions adopted pursuant to this Directive." Furthermore, the new Commission proposal for a Directive on the harmonisation of aspects of copyright and related rights in the Information Society of 1997 requires that "Member States shall provide appropriate sanctions and remedies in respect of infringements of the rights and obligations set out in this Directive."[515]

Since the above-mentioned Directives clearly show the differentiation between the harmonisation of prohibitions or safety measures and the enactment of sanctions of all kinds, these two distinct issues are going to be analysed separately in the following for the field of computer crime, too: The question in how far harmonised legal and technical measures, values and safety standards can be required by first pillar measures mainly focuses on the issue of finding an adequate legal basis and on the additional question as to which forms of computer crime can effectively be regulated on Community level in view of the principle of subsidiarity (infra 2). The second major issue is whether and to what extent the Community is also empowered to enact, or to require to enact, all kinds of sanctions on the basis of the respective legal basis found. Only the second issue is addressed by the numerous opinions in legal science referring to the EC's competence for "criminal law", mainly, however, in the context of protecting the Community's financial interests. Thus, it is going to be analysed in how far the principles established in the case law of the ECJ as well as by legal science with regard to the protection of the Community's budget can contribute valuable arguments also in the context of fighting computer crime by first pillar measures (infra 3).

2. Harmonising Non-Criminal Prohibitions and Duties

a. General Requirements of Article 100a of the Treaty

As described above, the EC can adopt measures relating to the fight against computer crime only if these measures can be based on an adequate legal basis of the EC Treaty. The actual choice of a legal basis is determined by the prerequisites of the empowering Treaty provision and by the objective aims pursued by the envisaged legal measures, which are subject to judicial

515 See supra chapter IV.C.4.a.

control. Thus, the decision for a certain legal provision must be based on objective criteria, in particular on the aim and the content of the legal measure to be adopted. The legal measure adopted must explicitly specify these criteria to allow such control of the legality of the measure by the ECJ.[516]

The Community has been active in a number of fields concerning the "information society", i.e. it has already adopted measures also in those areas which are largely affected by computer crime. Some of the documents published by the Community merely are non-binding recommendations or communications.[517] In those cases in which the Community adopted binding legal measures, it mostly used the instrument of directives, e.g. with respect to the deregulation of the telecommunications sector,[518] data protection,[519] as well as the legal protection of computer programs,[520] databases[521] or semiconductor topographies.[522] The legal basis of most of these directives has been Article 100a (1) EC Treaty, which was introduced to the EC Treaty in 1987 by the Single European Act and which empowers the Council and the European Parliament, in accordance with Article 189b EC Treaty and after consulting the Economic and Social Committee, to "adopt the measures for the approximation of the provisions laid down by

516 Cf. *Zuleeg*, in: Groeben/Thiesing/Ehlermann (eds.), Kommentar zum EU/EG-Vertrag, Article 3b, para. 15; ECJ, Judgement of 11 June 1991, Case C-300/89, (1991) ECR I-2867, para. 10; Judgement of 26 March 1987, Case 45/86, (1987) ECR 1493, para. 11.

517 Cf. for example Communication on harmful and illegal content on the Internet, COM(96) 487, 16 October 1996; Green Paper on the protection of minors and human dignity in the context of audiovisual and information services, COM(96) 483, 16 October 1996; as well as Commission Communication of the follow-up to the Green Paper on the protection of minors and human dignity in audiovisual and information services, including a Recommendation, COM(97) 570 final, 18 November 1997.

518 Following its Green Paper of 1987, the Community has, in the meantime, successfully abolished all exclusive and special rights of the former national telecommunications organisations including voice telephony as of 1 January 1998, using the instrument of directives based on Article 90 (3) of the EC Treaty. The subsequent re-regulation of the telecommunications sector, in particular the harmonisation directives establishing the principle of open network provision (ONP), have been based on Article 100a of the EC Treaty.

519 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, OJ L 281/31 of 23.11.1995.

520 Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs, OJ L 122/42 of 17.05.1991.

521 Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, OJ L 77/20 of 27.03.1996.

522 Council Directive 87/54/EEC of 16 December 1986 on the legal protection of topographies of semiconductor products, OJ L 24/36 of 27.01.1987.

law, regulation or administrative action in Member States which have as their object the establishment and functioning of the internal market." The Recitals of the respective Directives mentioned argue that differences in the legal protection of, e.g., computer programs[523] or databases[524] or different levels of data protection[525] in the various Member States endanger the functioning of the internal market. Similar arguments might also be valid in the field of computer crime, and the previous actions of the EC quoted above thus indicate that Article 100a of the Treaty might be a suitable legal basis also for the adoption of directives and regulations in the fight against computer crime.

Article 100a of the Treaty only permits the adoption of measures by qualified majority according to Article 189b of the EC Treaty. It allows both the enactment of directives and the adoption of regulations with the aim to harmonise Member States' provisions. However, according to a common Declaration of Member States on Article 100a of the EC Treaty adopted in 1985 at the time of signing the Single European Act, the Commission is asked to give priority to directives if the harmonisation involves the amendment of legislative provisions in one or more Member States.

Article 100a of the Treaty refers to the achievement of the objective of a genuine internal market as set out in Article 7a of the Treaty, i.e. an area without internal frontiers in which the free movement of goods, persons, services, and capital is ensured in accordance with the provisions of the Treaty. The term "internal market" implies a higher level of integration as opposed to the term "common market" used in Article 100 of the Treaty and thus includes the creation of homogeneous social and economic conditions beyond the mere exertion of the fundamental freedoms guaranteed by the EC Treaty.[526] Consequently, Article 100a aims at the abolition of the still existing barriers in the internal market,[527] but also allows harmonisation measures with the aim of creating equal conditions for effective competition. The European Court of Justice has confirmed that harmonising measures must be adopted in those fields in which different national rules create a risk of distorting competition.[528] As can be deduced from Article 100a (3), a

523 Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs, OJ L 122/42 of 17.05.1991.

524 Recital 3 of Directive 96/9/EC, see fn. 423.

525 Recital 7 of Directive 95/46/EC, see fn. 519.

526 *Langeheine*, in: Grabitz/Hilf (eds.), Kommentar zur Europäischen Union, Article 100a, para. 43.

527 *Langeheine*, in: Grabitz/Hilf, Kommentar zur Europäischen Union, Article 100a, para. 20.

528 ECJ, Judgement of 11 June 1991, Case C-300/89, (1991) ECR I-2867, para. 15.

harmonised high level of consumer protection in the internal market is also one of the objectives to be pursued by measures based on Article 100a.

Article 100a allows harmonisation measures with regard to the internal market only "save where otherwise provided" in the Treaty (Article 100a (1) cl. 1). This means that preference must be given to more specific legal bases if their field of application is concerned. However, in the field of computer crime, this relation between Article 100a and other possible legal bases contained in the EC Treaty does not create any major legal problems:

> To the degree that all kinds of commercial transactions, e.g. for the international sale of goods or the transfer of capital, are increasingly carried out via the Internet, international online services do not only fall within the ambit of the basic freedom to provide services, but also concern the free movement of goods and capital in the internal market. The internal market relevance as crucial criterion for opening the field of application of Article 100a of the Treaty thus cannot be denied at least as far as electronic commerce is concerned.[529]
>
> On the other hand, as the new online services exchanged between residents of various Member States constitute themselves services in the sense of Article 59 of the Treaty, a possible alternative legal basis for the adoption of measures against computer crime contained in the Treaty could be found in Articles 66 and 57 (2). On the basis of Articles 66 and 57 (2), the Community can adopt directives for the co-ordination of the provisions laid down by law, regulation or administrative action containing service-related restrictions. However, as this provision merely allows the "co-ordination" as opposed to the harmonisation of rules in the Member States which is necessary for an effective level of protection, as online services relate to the exchange of goods and capital and not merely services and as a variety of different aspects, e.g. consumer protection, can be considered in the context of Article 100a, Article 57 (2) of the Treaty cannot be considered a more specific norm than Article 100a for the field of online services. Preference should thus be given to this latter provision referring to the functioning of the internal market as a whole.

The analysis of paradigm shifts in the information society has shown that at least harmonised legal solutions are necessary in the field of international computer crime. However, in the context of Article 100a, the often international character of computer crime is not a sufficient legal criterion to justify the enactment of measures on this basis: Article 100a of the Treaty requires that computer crime, the consequent national rules existing to prevent it or – reversely – the lack of technical and legal countermeasures in the Member States somehow affect the functioning of the internal market, so that a harmonisation of these national provisions is necessary. This question of "internal market relevance" demands a careful analysis for each and every of the different forms of computer crime. Since the respective duties in the field of privacy protection and in the field of

529 Cf. in greater detail infra b.

intellectual property protection are already covered by existing EC directives,[530] the following analysis of EC competences under Article 100a of the Treaty will focus on the remaining areas of (non-criminal) duties and prohibitions in the fields of economic crime (infra b), illegal and harmful contents (infra c) as well as responsibility of online access and service providers (infra d).[531]

b. Article 100a with Respect to Economic Crime

The relevant forms of economic crime described above (i.e. hacking, computer sabotage, computer espionage, computer forgery and computer manipulations) can be committed both "offline" and "online". In view of the growing importance of online services and electronic commerce, the free flow of services, goods and capital among Member States and thus the functioning of the internal market can in particular be hindered if Member States either completely lack provisions relating to the protection against such online and offline manipulations concerning electronic commerce within the EC or if existing national provisions do not guarantee a harmonised level of protection:

If the authenticity and the security of electronic messages aiming at the conclusion of electronic contracts between parties in different Member States were not adequately ensured by Member States' provisions, this new form of commerce would be used less frequently, which would in turn reduce the transborder exchange of goods, services and capital in the internal market. Inadequate national rules with regard to the security of online commerce and electronic banking (e.g. low levels of protection against hacking, computer sabotage, computer espionage, computer forgery and computer manipulations) would mean a low level of consumer protection throughout the Community.

From the point of view of content and service providers such as banks, the existence of "computer crime havens" in the Community, i.e. differing levels of protection in the individual Member States, would mean unequal conditions for competition, favouring, on the one hand, in terms of costs for security measures those providers established in the Member State with the lowest level of protection. On the other hand, if electronic banking between a client and a bank located in different Member States entailed some risk of manipulation due to the lack of protection in the host Member State of the

530 See supra fn. 519 and 523.

531 The question whether there is also a power of the European Community to create criminal or administrative criminal sanctions with respect to the non-criminal prohibitions and duties will be discussed infra chapter VI.A.3.

bank with regard to the security of the transaction, the potential recipients of the service would stick to banks in their own Member State where more adequate protection is ensured, so that effective competition from other Member States would be hindered.

> The internal market relevance of national provisions relating to computer crime is less obvious when it comes to offences which do not involve a cross-border element neither in the commitment of the offence nor in the possible effects, e.g. when the offence does not involve a bank and a client located in different Member States, but merely offline computer fraud against a local ATM by using false access cards. The principle of subsidiarity might lead to the – premature – conclusion that such a scenario is of purely national character and that Member States can effectively deal with such offences on the national level alone. However, even national rules relating to purely domestic computer offences might have internal market relevance if they differ from each other to the effect that the different levels of protection lead to eventual distortions in the flow of services and goods in the Community: E.g. companies established in one Member State would cease to export computer programs into those Member States that do not have an effective legal protective system for computer software. Different legal regimes with respect to data protection would also provoke Member States' governments to restrict data flows to Member States with less developed protective systems, as is illustrated by export regulations for personal data in many privacy laws. These scenarios have effectively been dealt with by the Directive on the legal protection of computer programs[532] and by the Data Protection Directive[533] respectively. If e.g. due to the lack of adequate rules, telephone card manipulations led to such high damage amounts that manufacturers of public payphones would cease to export their technology to these Member States, this would represent a similar case of internal market relevance. In this area of offline manipulations, the Community has therefore got to carefully assess for each and every form of computer crime whether the criminal activity and differing national provisions for their prevention do indeed have internal market relevance. If this criterion is not fulfilled, the EC cannot legislate on the basis of Article 100a of the Treaty. If such internal market relevance exists, however, the Community would not be prevented from legislating on the basis of Article 100a by the principle of subsidiarity, because the necessary harmonisation of Member States' laws could not be achieved without Community action.

These scenarios indicate that differing or lacking provisions with regard to the security of online services and electronic commerce clearly have internal market relevance especially with regard to market distortions, and that a corresponding harmonisation of national rules could thus be based on Article 100a of the Treaty. In a directive based on this Treaty provision, the recitals of which would have to state the above-mentioned considerations as objective aims of the Community's measure, the EC could therefore require Member States, inter alia,

532 Cf. above fn. 523.

533 Cf. above fn. 519.

- to protect the security of European computer networks against computer-related crime by adequate prohibitions especially against hacking, espionage, sabotage and manipulations,
- to create effective rules concerning digital signatures protecting the integrity and authenticity of electronic messages as well as general rules allowing the use of encryption technologies to protect the secrecy of electronic data,534
- to create certain minimum standards of security (e.g. for privacy protection) in European computer networks.

As a consequence, e.g., a future directive on electronic commerce could require Member States to prohibit certain acts infringing the security of electronic commerce such as hacking, sabotage, espionage, forgery and manipulations. Based on the above described differentiation between mere prohibitions and sanctions for infringing these prohibitions, it will be discussed below whether or not the respective directive could also cover the demand for adequate sanctions against the infringement of these prohibitions.

c. Article 100a with Respect to Illegal and Harmful Contents

In principle, even such online services which might contain harmful or illegal contents such as the dissemination of erotic pictures or defamatory statements principally fall within the ambit of Article 59 of the Treaty if the recipient and the provider of the service are located in different Member States and if the service is offered in return for some remuneration. The situation is comparable to cross-border TV broadcasting, which the ECJ qualifies as a service in the sense of Article 59 of the Treaty and which the Community is thus empowered to regulate.[535] It has been illustrated above in chapter III.E.1 that in the field of communication offences, national standards as to what contents are permissible (and consequently national criminal norms) differ considerably. This divergence of national standards

534 Whereas asymmetric encryption (this type of encryption requires the existence of a secret and a public key) which is exclusively used to create so-called digital signatures cannot prevent manipulations on the plain text itself but is a means to control whether such manipulations have taken place (via the comparison of a checksum), digital symmetric or asymmetric encryption used to encode plain text is also a means that could effectively prevent the alteration of electronic data, e.g. the forgery of online documents such as contracts.

535 ECJ, Judgement of 30 April 1974, Case 155/73, (1974) ECR, p. 428, para. 6; Judgement of 18 March 1980, Case 52/79, (1980) ECR, p. 833, at p. 855, para. 8; also cf. *Kugelmann*, Der Rundfunk und die Dienstleistungsfreiheit des EWG-Vertrags, pp. 60 et seq.

and criminal norms can lead to severe distortions in the functioning of the internal market:

The classic example of an online service that might lead to a conflict in the internal market is an online journal with erotic pictures or with sensible political propaganda that is legal in the originating Member State A, but which is accessible and delivered to another Member State B, where these pictures or statements are considered illegal pornography or hate speech. In these cases, national prosecution authorities will usually apply their procedural and substantial national criminal law provisions, e.g. by asking access or service providers to block access to that particular service on the basis that its dissemination or receipt constitutes a criminal offence in that Member State.[536] In view of the fundamental freedom of the free flow of services in the internal market, the application of these national criminal rules and investigation measures in the Member States where the service is requested creates considerable legal problems:

> EC law contains the general principle that providers of services shall be controlled by the Member State in which they are established.[537] The European Court of Justice has ruled that a service provider (e.g. an insurance company) established and licensed in one Member State can be submitted to further non-discriminatory regulations in another Member State only if these restrictions are justified in the general interest and only if this general interest has not yet been taken into consideration by the host Member State that has issued a licence.[538] The publishers of the particular online journal who are legally established in their home Member State might claim that the blocking is not justified in the general interest and that their freedom to provide services is thus violated. Another Treaty provision on grounds of which Member States could block services that they consider harmful or illicit is the public policy proviso of Article 56 (1) of the Treaty. Both the terms "public policy" and "general interest" are so imprecise and open for interpretation that Member States could easily be tempted to apply their more restrictive national criminal laws. This would represent an infraction of Article 59 of the EC Treaty and thus an obstacle for the functioning of the internal market in each and every case in which the Member States' interventions could neither be justified in the general interest nor by Article 56 (1) of the Treaty.

---

536 For an example of such a case cf. above chapter II.C. For the field of television, a comparable development can be observed in the (non-EU) country of Norway, which limits access to cable TV programs of Swedish television stations due to the more generous pornography legislation in Sweden. See above chapter III.D.1.c.

537 *Troberg*, in: Groeben/Thiesing/Ehlermann (eds.), Article 57, para. 15.

538 ECJ, Judgement of 4 December 1986, Case 205/84, (1986) ECR 3755, para. 27. A special case is given if a broadcasting organisation that is established in one Member State directs all or most of its activity to the territory of another Member State, and the choice of establishment was made with a view to evading the legislation that would have applied to the organisation had it been established on the territory of this latter Member State. For these cases, the ECJ has constantly held that the latter Member State retains the right to take measures against such an organisation; cf. ECJ, Judgement of 3 December 1974, Case 33/74, (1974) ECR, p. 1299 and Judgement of 5 October 1994, Case C-23/93, (1994) ECR, p. I-4795.

The need for harmonisation measures in order to create a common level of accepted contents preventing such interventions by individual Member States thus becomes obvious. Moreover, a criminal prosecution of the managers of service provider companies which offer lawful services in one Member State in another Member State that considers these services unlawful would definitely represent a distortion of competition and would not only lead to a reduction of the cross-border exchange of these particular services, but might reduce the overall volume of online services in the internal market due to the uncertain legal situation. Consequently, the question whether divergent national criminal norms relating to the dissemination of, e.g., pornographic or racist content are of internal market relevance can certainly be answered in the affirmative. The harmonisation of these differing national criminal norms could thus be based on Article 100a of the EC Treaty, aiming at the elimination of potential obstacles in the internal market and an increased marketability of online services as a whole by setting minimum standards for the particular online services in question.

However, as such a harmonisation of Member States' rules with regard to communication offences would not require the setting of harmonised technical safety regulations or prohibitions, but would – indirectly – rather imply the harmonisation of cultural standards as to what contents are still permissible, Member States could show a certain resistance against the harmonisation of these moral standards and values at Brussels by supranational measures. From the legal point of view, this resistance could be neglected; once more, there is an obvious parallel of online services and television: As in the case of television, online services do have a cultural, but above all also a strong economic aspect, so that the definition of "services" in the sense of Article 59 of the Treaty is undoubtedly fulfilled irrespective of this undeniable cultural aspect.[539] Consequently, the Directive 89/552/EEC on the harmonisation of Member States rules concerning TV broadcasting (commonly known as "Television Without Frontiers"),[540] of which Article 22 clearly regulates cultural aspects with regard to the

539 Cf. the references in fn. 535 above.

540 Council Directive 89/552/EEC of 3 October 1989 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the pursuit of television broadcasting activities, OJ L 298/23 of 17.10.1989; recently amended by Directive 97/36/EC of the European Parliament and of the Council of 30 June 1997 amending Council Directive 89/552/EEC of 3 October 1989 on the co-ordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the pursuit of television broadcasting activities, OJ L 202/60 of 30.07.1997.

protection of minors and public order,[541] can serve as a model legal provision for the prohibition of indecent and harmful online activities, too: An EC Directive harmonising national prohibitions could explicitly require Member States to prohibit online services containing information which might seriously impair the physical, mental or moral development of minors, in particular online services that involve pornography or gratuitous violence or which contains hate speech or racist, national-socialist and fascist propaganda.

In order to really achieve a common level of protection throughout the Community and to avoid the kind of market distortions described above, a future directive on the harmonisation of Member States' legal provision with respect to online communication offences might possibly have to regulate the respective prohibitions in greater detail than the "Television Without Frontiers"-Directive, precisely specifying (by way of harmonised definitions) which contents are still permissible and which are illicit in European computer networks. The prohibitions could be specified e.g. with respect to child pornography, xenophobia, racism as well as other illegal or harmful contents. On the other hand, the aim to increase the marketability of online services in the internal market and to avoid market distortions does not necessarily require unified European solutions (which could only be achieved by an EC regulation), but merely harmonised ones: In view of the principle of proportionality, similar (and not identical) national provisions resulting from a harmonising directive based on Article 100a of the Treaty and guaranteeing a harmonised (and not unified) level of accepted standards in Europe would probably be sufficient to reach the desired aims, thus leaving enough room for national particularities that do not affect this common level of protection. On the basis of the previous work carried out in this field, a European working group should specifically analyse the diverging national criminal norms and underlying cultural aspects and then suggest a common European standard as well as concrete provisions of a future directive.

In any case, the harmonisation of standards with regard to illegal and harmful contents in European computer networks by a directive based on Article 100a of the Treaty remains as much a legal as a political question. In case that a directive proposal in this field is not possible or advisable for political reasons, the respective prohibitions should be dealt with in the

541 Article 22 (1) of Council Directive 89/552/EEC as amended provides that "Member States shall take appropriate measures to ensure that television broadcasts by broadcasters under their jurisdiction do not include any programs which might seriously impair the physical, mental or moral development of minors, in particular programs that involve pornography or gratuitous violence."

context of third pillar action by joint actions or conventions in which Member States can agree on a common level of accepted contents.[542]

d. Article 100a with Respect to the Responsibility of Online Access and Service Providers

It was shown above that the international nature of online services makes it very difficult to legally pursue the authors of illicit and harmful contents. Therefore, the harmonisation of prohibitions with respect to illegal and harmful contents, which is exclusively addressed towards the authors of such information (i.e., in other terms, "content providers") would not be complete without the regulation of further responsibilities for such contents, i.e. the responsibility of online access and service providers storing this information on their servers.

Germany has been the first Member State to set up explicit rules for such responsibilities of online access and service providers.[543] If such rules differed among the Member States, providers would tend to establish themselves in Member States where the national law does not provide for a severe legal responsibility for contents stored. Access and service providers established in Member States with more restrictive rules both for authors of illegal and harmful contents (content providers) and with respect to the responsibility of access and service providers would constantly be confronted with the above-described requests by prosecution authorities to block the illegal contents and might also be exposed to legal risks. They would thus clearly be in a disadvantageous position as opposed to their competitors in other Member States, which would undoubtedly represent a distortion of competition in the internal market.

Moreover, if the EC agreed on harmonised rules for online contents, a common level of protection could only effectively be reached if a certain responsibility of online access and service providers for these contents existed, too: In many cases, the factual situation would be such that the authors of the illegal contents cannot be effectively pursued and that efficient prosecution measures can only be taken with respect to the access and service providers. Therefore, the harmonisation of the responsibility of online access and service providers is the indispensable completion to the harmonisation of contents discussed above.

Consequently, regulations on such responsibility of online access and service providers could be included in a directive based on Article 100a of

542 Cf. infra chapter VI.B.

543 Cf. above chapter III.E.2.

the Treaty in order to avoid the above-mentioned market distortions and to ensure the effectiveness of the harmonisation of contents. Harmonised rules for the responsibility of access and service providers are not only required with respect to criminal law provisions and pornography, hate speech and libel, but also with respect to the liability for copyright infringements. In order to guarantee harmonised solutions without restricting the free flow of services in the internal market and without actually regulating concrete criminal sanctions, a future directive could be based on the following principles:

- providers should be responsible in accordance with general laws for their own content, which they produce or which they make available for use,
- providers should not be responsible for any third-party content which they make available for use on their servers unless they have knowledge of such content and are technically able and can reasonably be expected to prohibit the storage of such content,
- finally, providers should not be held responsible for any third-party content to which they *only provide access* (unless they contravene concrete and non-appealable blocking orders).[544]

e. Article 100a (4) with Respect to Higher National Levels of Protection

The harmonisation of Member States' rules concerning duties and prohibitions in the field of economic crime and communication offences aims at minimum standards for the abolition of barriers to the free flow of information and the transborder exchange of online services in the internal market. This harmonisation is especially needed in those cases in which Member States completely lack respective provisions. However, it is unclear which level of protection Member States can agree on in the Council when a future harmonising directive is to be adopted on the basis of Article 100a of the Treaty.

In some Member States, legal provisions might be in force that guarantee a higher level of protection and some Member States might want to continue to apply these stricter national rules. This could especially be the case in the field of communication offences reflecting specific national morals and standards of decency, on the basis of which individual Member

544 For more details of the technical basis of this proposal see *Sieber*, Kontrollmöglichkeiten zur Verhinderung rechtswidriger Inhalte in Computernetzen, (1997) Computer und Recht, pp. 581 et seq. and pp. 653 et seq.

States could require, e.g. the blocking of services considered harmful or illegal in that particular Member State. According to Article 100a (4) cl. 1 of the Treaty, a Member State that deems it necessary to apply, after a harmonisation measure by the Council has been adopted by qualified majority on the basis of Article 100a, national provisions on grounds of major needs referred to in Article 36 of the Treaty, must notify the Commission of these provisions. According to Article 100a (4) cl. 2 of the Treaty, the Commission shall confirm these provisions after having verified that they are not a means of arbitrary discrimination or a disguised restriction of trade between Member States. The major needs referred to in Article 36 include, in particular, public morality and public policy. Therefore, a Member State deeming the harmonised Community level of protection too low could continue to apply national rules reflecting e.g. certain more restrictive national standards with respect to the dissemination of pornography on the basis of Article 100a (4) cl. 1 of the Treaty, provided that the Commission has confirmed the provisions according to Article 100a (4) cl. 2 of the Treaty.

Critics might argue that because of this opt-out possibility offered by Article 100a (4) of the Treaty, the adoption of a harmonising directive would be futile, because the differences among the national prohibitions would continue to exist. However, the advantage of such a harmonising directive would first of all be the introduction of a minimum level of protection throughout the Community. The theoretical danger that individual Member State arbitrarily maintained inadequately strict national rules would be countered by the Commission's control powers under Article 100a (4) cl. 2. Moreover, if Member States were of the opinion that another Member State made improper use of the powers provided for by Article 100a (4), they could bring the matter directly before the ECJ (Article 100a subs. 4 cl. 3), so that there are efficient control mechanisms preventing the emergence of too restrictive national rules arbitrarily affecting the flow of online services in the internal market.

3. Competences for Sanctions?

The analysis above has shown that the EC is empowered, on the basis of Article 100a of the EC Treaty, to issue directives and – theoretically – also regulations harmonising Member States' legal prohibitions and duties as well as technical standards with respect to many aspects of computer crime. The subsequent question to answer is now whether and to what extent the EC is also competent to regulate how infractions against these legal duties and prohibitions should be sanctioned. This would mean that the EC would

create – directly or indirectly – a complete criminal norm which usually consists of a prohibitive and a sanctioning part.

The Community's competence to adopt supranational criminal law provisions, less intensive provisions of administrative criminal law or other non-criminal sanctions in directives or in directly applicable regulations according to Article 189 (2) of the EC Treaty has been widely discussed in European legal science with respect to the protection of the Community's financial interest. In the following, it is going to be analysed if and how the EC can create supranational criminal sanctions (infra a) or administrative criminal sanctions (infra b) by way of issuing a regulation or whether it can only require Member States to adopt such sanctions by way of a directive (infra c). In this analysis, the principles established in the discussion on the protection of the Community's financial interest will be transferred to the field of computer crime.

a. Supranational Criminal Sanctions in Regulations

The EC Treaty in its present form does not explicitly address the issue of competences for criminal law. However, both the history of European unification and the intentions of the founding members of the EC clearly speak against the assumption of such competences. In addition to this, the general constitutional principles of democracy and due course of law, especially the principle of "nullum crimen sine lege", have served as strong arguments against an EC competence for criminal sanctions. It has been argued that in all Member States, certain provisions of constitutional law, such as Articles 23 and 24 (1) of the German Basic Law (Grundgesetz), bind the conferral of sovereign rights to certain "irrevocable parts"[545] of the national constitutional structure, a major part of which are the principles of democracy and due course of law.[546] These principles and the demand for a clear democratic authorisation are especially important since criminal sanctions are the most severe intrusion of state powers in civil liberties. It was often questioned whether the EC could fulfil these fundamental requirements, mainly because of the fact that the Council of Ministers and the Commission have no direct democratic authorisation and because a traditional separation of powers does not exist within the EC. After the

545 Such is the expression used by the Bundesverfassungsgericht, cf. Entscheidungssammlung des Bundesverfassungsgerichts, Vol. 58, p. 1, at p. 40.

546 The new Article 23 of the Basic Law, which has been introduced with regard to the Maastricht Treaty in 1993, expresses this clearly once again: According to Article 23 (1) cl. 1, the European Union has to observe the "democratic, federal and social principles as well as the principle of the rule of law". According to Article 23 (1) cl. 3, the existence of these principles is protected by Article 79 (2) and (3) of the Basic Law.

Maastricht Treaty introduced the co-decision procedure (Article 189b of the EC Treaty) in 1993, which is applicable for all measures based on Article 100a of the EC Treaty, as well as the control powers vis-à-vis the Commission according to Article 144 of the EC Treaty, the position of the European Parliament has been considerably strengthened. The Parliament could now block the adoptions of EC measures intending to create criminal law sanctions on the basis of Article 100a of the EC Treaty. Still, the prevailing and as yet undisputed opinion in legal science holds that the EC has no genuine law making competence for criminal law:[547] A different conclusion could only be reached for specific fields after the entry in force of the Treaty of Amsterdam, which provides for special competences with respect to fraud against the financial interests of the Community in the new Article 280 (formerly Article 209a) of the Treaty.[548] However, this special provision only refers to the protection of the Community's financial interests and is not applicable in the field of general computer crime.

b. Supranational Criminal Administrative Law in Regulations

The historic and systematic interpretation of the EC Treaty does not unveil convincing reasons for or against a general competence for the enactment of less severe, merely administrative penal sanctions such as fines for regulatory offences. Likewise, it is not fully clear in how far national constitutions prohibit the conferral of powers for adopting certain less intense sanctions of administrative criminal law nature, the more so since some sort of parliamentary control exists at EC level. The EC Treaty itself explicitly provides for the possibility to adopt administrative fine provisions in the field of competition law on the basis of Article 87 (2) (a) of the EC Treaty, which enables the Council to adopt regulations and directives that include administrative fines and coercive enforcement penalties. On the basis of this vague general authorisation of Article 87 of the EC Treaty, the

547 See, for this, *Dannecker*, Strafrecht der Europäischen Gemeinschaft, in: Eser/Huber (eds.), Strafrechtsentwicklung in Europa, 1995, p. 2004; also cf. the references quoted above in fn. 507. This is correct from the constitutional point of view in so far as the European Parliament still does not have comprehensive legislative powers by virtue of which it could, e.g., abolish an existing legal measure.

548 Cf. Article 280 (4) of the EC Treaty as amended by the Treaty of Amsterdam: "The Council, acting in accordance with the procedure referred to in Article 251, after consulting the Court of Auditors, shall adopt the necessary measures in the fields of the prevention of and fight against fraud affecting the financial interests of the Community with a view to affording effective and equivalent protection in the Member States. These measures shall not concern the application of national criminal law or the national administration of justice."

Council has enacted various regulations[549] containing "non-criminal" sanctions allowing for administrative fines of up to ECU one million or up to ten percent of the annual turn-over of the company in question. In some cases these "non-criminal" sanctions were as high as ECU 12 million in the case of a single company and ECU 75 million in the case of a single cartel.[550]

The crucial question is whether the EC is competent, by way of adopting a regulation, to enact new, global, supranational regulatory sanctions for the violation of harmonised prohibitions outside of the scope of application of Article 87 of the EC Treaty, i.e. in fields in which the EC Treaty merely allows, as in Article 100a of the EC Treaty, the adoption of all necessary "measures". The fact that Article 87 of the EC Treaty explicitly provides for the power to enact administrative fines could lead to the conclusion that administrative sanctions cannot be based on Treaty provisions which do not explicitly mention such power. In the field of irregularities to the detriment of the Community's budget, the Council based a framework regulation[551] setting up common rules with respect to administrative measures and penalties on Article 235 of the EC Treaty, which signifies that even the Council itself did not find another appropriate legal basis for the enactment of a regulation containing administrative criminal sanctions. From the point of view of constitutional law, a more precise legal basis than provided by the general term "measures" in Article 100a of the Treaty would be desirable for the enactment of administrative sanctions in a regulation again mainly because of the principle of "nullum crimen sine lege". On the other hand, the fact that administrative criminal sanctions are less intense in their possible infringements of citizens' rights might allow a somewhat more lenient application of the principle of clarity.[552] Once again, the discussion is as much of political as of legal nature: At present, it seems very unlikely that the Member States could agree on a Council regulation creating new administrative criminal law provisions, simply because the political time for genuine supranational sanctions has not yet come. Moreover, computer crime mostly stands for serious breaches of law which deserve to be

549 See Regulation No. 17, (1962) OJ 204/62 of 21.12.1962; Regulation No. 1017/68, (1968) OJ L 175/1 of 23.07.1968; see, for this, *Oehler*, Internationales Strafrecht, 1983, p. 562 et seq.

550 See, for this, *Dannecker/Fischer-Fritsch*, Das EG-Kartellrecht in der Bußgeldpraxis, 1989, p. 133 et seq.

551 Council Regulation No. 2988/95 of 18 December 1995 on the protection of the European Communities' financial interest, OJ L 312/1 of 23.12.1995.

552 See, for this system of "gradation", Bundesverfassungsgericht, Entscheidungssammlung des Bundesverfassungsgerichts, Vol. 75, p. 329, at 342; *Kunig*, Zur "hinreichenden Bestimmtheit" von Norm und Einzelakt, (1990) Jura, p. 495 et seq.

sanctioned by criminal law and would thus not be treated adequately as a mere regulatory offence.[553]

c. Criminal Sanctions of National Law Required by Directives

Since the Community is, at least for the time being, not empowered to create criminal sanctions in a directly applicable regulation based on Article 100a of the Treaty, the question arises whether and to what extent the EC can require Member States, via the instrument of directives according to Article 189 (3) of the EC Treaty, to adopt *national criminal law sanctions* for infractions against the harmonised prohibitions described above.

The EC's power to adopt binding directives according to Article 189 (3) of the EC Treaty has substantially influenced and continues to influence national legislation in all fields of law. EC directives also have considerable influence on criminal law, though this influence is not always visible. This is especially true when EC directives influence civil and administrative law to which criminal law refers to[554] and when EC directives guarantee fundamental liberties which cannot be restricted by national criminal law.[555]

With respect to the competence to oblige Member States to implement directives requiring the enactment of national criminal law sanctions, the above mentioned constitutional concerns are not valid. The directives are addressed only to the Member States,[556] and even if the directives require

553 However, as in the context of criminal sanctions, the above-mentioned constitutional concerns do not apply if Member States enact administrative sanctions in the implementation of a directive harmonising certain duties or prohibitions. Such administrative fines might be sufficient for the effective application of some harmonised prohibitions and duties, e.g. the requirement for service providers to offer adequate safety measures. If this were the case, the principle of proportionality would prevent Member States from enacting more intense criminal sanctions for the respective infractions.

554 E.g. accounting rules or company, tax, food, drug, environmental, and agricultural law.

555 See ECJ, Judgement of 4 October 1991, Case C-159/90, (1991) ECR, p. I-4685. EC directives do not only directly bind the national legislator, national administration and the national courts. They also influence the interpretation of national rules as a consequence of the duty to interpret national legislation consistently with the provisions of relevant directives (cf. ECJ, Judgement of 13 November 1990, Case C-106/89, (1990) ECR, p. I-4135). An interpretation of national laws which is consistent with relevant directives can clearly be detected in the case-law of the German Federal High Court of Justice in criminal matters. See Bundesgerichtshof, Entscheidungssammlung des Bundesgerichtshofs, Vol. 37, pp. 168 et seq., at 174 et seq.; Bundesgerichtshof, (1991) Neue Zeitschrift für Strafrecht, pp. 282 et seq., at 283; *Thomas*, Die Anwendung europäischen materiellen Rechts im Strafverfahren, (1991) Neue Juristische Wochenschrift, pp. 2233 et seq., at p. 2235.

556 ECJ, Kolpinghuis Nijmegen, Case 80/86 (1987) ECR, pp. 3969, at p. 3986.

the adoption of national criminal sanctions, these national laws have the direct democratic authorisation of the national legislators.[557] The decisive question that remains is only how detailed the EC may lay down national criminal provisions. In this regard, the "Greek-Corn-Decision" of the European Court of Justice places the Member States, with respect to Article 5 of the EC Treaty, under the obligation to "take all necessary measures in order to have the EEC laws remain effective". In addition, the ECJ proclaimed that "the Member States, which retain the choice between the various forms of penalisation, must ensure that infringements on EEC law will be punished by similar substantive and procedural rules as would apply to the infringement of comparable national law, considering the necessity for an effective, proportional, and deterring sanction".[558] In the meantime, the Maastricht Treaty has explicitly incorporated the principles established in this court ruling in Article 209a EC Treaty with respect to the protection of the financial interests of the EC.[559]

As a general consequence of this ruling and taking into account the two fundamental EC law principles of "effet utile" on the one hand and the principle of proportionality on the other hand, a general rule can be established with regard to the EC's competence to adopt directives requiring Member States to enact criminal sanctions: The EC is competent to require the Member States to adopt criminal sanctions for infractions against Community-wide harmonised duties and prohibitions in all cases, but only in those cases, in which such criminal sanctions are necessary to guarantee the effective application of the prohibitions and duties harmonised by EC law. The EC can require the enactment of national criminal law sanctions in such detail, but only in such detail, as is necessary to ensure such effective application of EC law in order to achieve the aims of the Treaty in accordance with the legal provision of the Treaty on which the directive is based, i.e. Article 100a of the Treaty.

However, even though the legal situation would thus allow the adoption of directives requiring the enactment of national criminal sanctions, it is necessary to take a look at the EC's political disposition to do so. Criminal

557 See for this, *Dannecker*, Strafrecht der Europäischen Gemeinschaft, in: Eser/Huber (eds.), Strafrechtsentwicklung in Europa, 1995, pp. 2023 et seq.

558 See ECJ, Cases 68/88, (1989) ECR, pp. 2965 et seq., at pp. 2984 et seq.

559 After the coming into force of the Amsterdam Treaty, this protection of the financial interests of the Community will be addressed by Article 280 of the EC Treaty, which stipulates that Member States must take the same measures against fraud to the detriment of the Community's financial interest as they take against fraud against their own financial interests. Cf. above fn. 548.

law always is political law.[560] Up to now, there are no precedents of a directive explicitly requiring the adoption of precisely defined criminal sanctions by the Member States. E.g., even in the field of money laundering, where the creation of criminal law provisions had already been agreed on by the Vienna Convention of 1988[561] and where Germany eventually enacted Section 261 Criminal Code, the corresponding Council Directive 91/308/EEC on Money Laundering[562] does not expressly demand the adoption of criminal law provisions, but merely provides that Member States have to adopt "appropriate measures" in order to ensure the full application of all provisions of the Directive (Article 14). Plans to require Member States to actually enact a genuine criminal norm were highly disputed and were eventually not pursued by the Community.[563] Another example is the field of the protection of the financial interests of the Community: The creation of a directive was long discussed in this field, but eventually only third pillar action was taken by Member States agreeing on the 1995 Convention on the protection of the financial interests of the Community.[564] This result of intergovernmental co-operation was then accompanied by a 1995 Framework Regulation with respect to "non-criminal" sanctions.[565] Further reaching actions are the above described 1995 EC Data Protection Directives and the 1997 Commission proposal for a Directive on the harmonisation of certain aspects of copyright and related rights in the information society which require Member States to enforce the underlying duties and prohibitions by appropriate sanctions.[566] In conclusion, the Council seems to show no political disposition to require Member States

560 Cf. the statement of *Tiedemann*, Die Europäisierung des Strafrechts, in: Kreuzer/Scheuing/Sieber (eds.), Die Europäisierung der mitgliedstaatlichen Rechtsordnungen in der Europäischen Union, p. 134: "Strafrecht ist nun einmal stärker als andere Rechtsmaterien Ausdruck nationaler Souveränität, auf die man nur ungern auch nur teilweise verzichtet, und Strafrecht ist damit zumindest in weiten Teilen politisches Recht, das eine besonders starke Bindung an Tradition und Wertebewußtsein, aber auch an Emotionen und Ängste aufweist."

561 UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances of 19 December 1988, D/Conf. 82/15.

562 Council Directive 91/308/EEC of 10 June 1991 on prevention of the financial system for the purpose of money laundering, OJ L 166/77 of 28.06.1991; cf. above fn. 513.

563 Cf. *Tiedemann*, Europäisches Gemeinschaftsrecht und Straftrecht, (1993) Neue Juristische Wochenschrift, pp. 23 et seq., at p. 26.

564 OJ C 316/48 of 27.11.1995; cf. above fn. 501.

565 Council Regulation No. 2988/95 of 18 December 1995 on the protection of the European Communities' financial interests, OJ L 312/1 of 23.12.1995.

566 See supra chapter VI.A.1.b.

by way of directives to enact precisely described criminal law provisions.[567] However, there are already considerable precedents of directives requiring Member States to enforce specific (non-criminal) duties and prohibitions by "sanctions".

The consequence of these considerations is this: If the EC were to require Member States, e.g., in a future directive on electronic commerce and/or on illegal and harmful contents, to prohibit certain activities in computer networks by national law, it could also require Member States to create adequate measures or even "sanctions" enforcing these prohibitions.

4. Conclusions

The EC can enact directives on the harmonisation of Member States provisions with respect to

a. acts to be prohibited and sanctioned by Member States in order to guarantee the security of electronic commerce (e.g. with respect to hacking, espionage, sabotage, manipulations)
b. acts to be prohibited and sanctioned by Member States in order to reach common standards throughout the Community with regard to illegal and harmful contents, but also in order to avoid further-going restrictions of international data flow by Member States (which go beyond a list of illegal acts as defined by EC law)
c. the (civil, administrative and criminal) responsibility of online access and service providers for illegal and harmful contents.[568]

Demands for a harmonisation or unification of criminal law provisions that go beyond this level, should – at least for political reasons – be dealt with by third pillar measures. This is especially important with respect to a more detailed regulation of the sanctions and with respect to criminal procedural law for which the first pillar does not provide competences.

567 The reason for this reluctance must partly also be attributed to the fact that third pillar action represents an adequate alternative to directives as long as the parties to a convention actually comply with the duties they consented to.

568 The harmonisation of the responsibility of online access and service providers has special priority since in this area, most Member States have really started not yet to adopt national legislation. Therefore, the European Community should deal with this question in a priority action before further-going national legislation will render a harmonisation more difficult.

B. Actions Covered by the Third Pillar

Actions under the third pillar of the EU Treaty with respect to computer crime create less problems for the EU competences as actions under the first pillar. The EU Treaty signed in Maastricht on 7 February 1992 provided new rules in the K Articles of Title VI on co-operation in the fields of justice and home affairs (infra 1). The Treaty of Amsterdam amending the Treaty establishing the European Union signed on 2 October 1997 (and not yet ratified) will considerably extend these provisions on police and judicial co-operation in criminal matters (infra 2). Both Treaties enhance the Council's competences for actions in the field of computer crime (infra 3).

1. Actions under the Maastricht Treaty

According to Article K.1 of the Maastricht Treaty, Member States shall, for the purposes of achieving the objectives of the Union, in particular the free movement of persons, regard the following areas as matters of common interest without prejudice to the powers of the European Community:

"(5) combating fraud on an international scale in so far as this is not covered by (7) to (9); ...

(7) judicial co-operation in criminal matters; ...

(9) police co-operation for the purposes of preventing and combating terrorism, unlawful drug-trafficking and other serious forms of international crime, including if necessary certain aspects of customs co-operation, in connection with the organisation of a Union-wide system for exchanging information within a European Police Office (Europol)."

With respect to these aims, Article K.3 empowers the Council (using measures generally adopted by a majority of two thirds) to:

"(a) adopt joint positions and promote, using the appropriate form and procedures, any cooperation contributing to the pursuit of the objectives of the Union;[569]

(b) adopt joint action in so far as the objectives of the Union can be attained better by joint action than by the Member States acting individually on account of the scale or effects of the action envisaged; it may decide that measures implementing joint action are to be adopted by a qualified majority;[570]

569 Joint positions are a new co-operation instrument in the area of home affairs introduced by the Maastricht Treaty. There is a controversy in legal science about their commitment effect for the Member States (see *Hailbronner/Klein/Magiera/Müller-Graff*, Handkommentar zum Vertrag über die Europäische Union (EUV/EGV), Article K, VII), which until now has not been solved.

570 The instrument of joint action, too, has been introduced by the EU Treaty. The Member States mostly are of the opinion that joint actions are binding for them. This conclusion is based on

(c) without prejudice to Article 220 of the Treaty establishing the European Community, draw up conventions which it shall recommend to the Member States for adoption in accordance with their respective constitutional requirements."[571]

2. Actions under the Amsterdam Treaty

After the ratification of the Treaty of Amsterdam signed on 2 October 1997, the provisions on police and judicial co-operation in criminal matters of Maastricht Treaty (Title VI) will be considerably amended and renumbered. The new Article 29 (ex-Article K.1) establishes that "the Union's objective shall be to provide citizens with a high level of safety within a area of freedom, security, and justice". According to Article 30 (ex-Article K.2), "common action in the field of police co-operation shall include ... operational co-operation between the competent authorities, including the police, customs and other specialised law enforcement services of the Member States in relation to the prevention, detection and investigation of criminal offences ..." According to Article 31 (ex-Article K.3), common action on judicial co-operation in criminal matters shall include:

"(c) ensuring compatibility in rules applicable in the Member States, as may be necessary to improve such co-operation;

(d) preventing conflicts of jurisdiction between Member States;

(e) progressively adopting measures establishing minimum rules relating to the constituent elements of criminal acts and to penalties in the field of organised crime, terrorism and illicit drug trafficking."

Moreover, Article 32 (ex-Article K.4) provides that "the Council shall lay down the conditions and limitations under which the competent authorities referred to in Articles K.2 and K.3 may operate in the territory of another Member State in liaison and in agreement with the authorities of that State."

Article 34 (ex-Article K.6) defines the types of action possible within the third pillar. It abolishes the former joint actions under the Maastricht Treaty and replaces it by framework decisions which – similar to the directives of

---

Article J.3 (4) of the Maastricht Treaty, in which the committing effect of joint actions is explicitly regulated for the common foreign and security policy. Joint actions are also published in part L of the Official Journal and include provisions about their entry into force (see *Hailbronner/Klein/Magiera/Müller-Graff*, Handkommentar zum Vertrag über die Europäische Union (EUV/EGV), Article K, VII.4).

571 Conventions are not binding. They become binding only with the Member States' consent (see *Hailbronner/Klein/Magiera/Müller-Graff*, Handkommentar zum Vertrag über die Europäische Union (EUV/EGV), Article K, VII.5).

the first pillar under Article 189 (3) EC Treaty – are binding for the Member States as to the result which shall be achieved but will leave the national authority the choice of form and methods. As a consequence, the Amsterdam Treaty provides, in the new Article 34 (ex-Article K.6), for four types of measures: Acting unanimously on the initiative of any Member State or of the Commission, the Council may:

"(a) adopt common positions defining the approach of the Union to a particular matter;

(b) adopt framework decisions for the purpose of approximation of the Member States. Framework decisions shall be binding upon the Member States as to the result to be achieved but shall leave the national authorities the choice of form and methods. They shall not entail direct effect;

(c) adopt decisions for any other purpose consistent with the objectives of this Title, excluding any approximation of the laws and regulations of the Member States. These decisions shall be binding and shall not entail direct effect; the Council, acting by a qualified majority, shall adopt measures necessary to implement those decisions at the level of the Union;

(d) establish conventions which it shall recommend to the Member States for adoption in accordance with their respective constitutional requirements. Member States shall begin the procedures applicable within a time limit to be set by the Council."

3. Consequences for Council Actions in the Field of Computer Crime

Following the findings and arguments above, there is no doubt that fighting international computer crime falls under Article K.1 (5), (7), (9) of the EU Treaty (especially with under the terms combating fraud at an international scale; traditional corporation in criminal measures; police corporation for the purposes of preventing other serious forms of international crime). The competence of the Council will be even broader under the new Articles 29 (ex-Article K.1), 30 (ex-Article K.2) and 31 (ex-Article K.3) revised by the Amsterdam Treaty (especially with respect to: providing a high level of safety within an area of relative freedom, security and justice; operational police corporation; insuring compatibility of rules applicable in the Member States, which may be necessary to improve co-operation; preventing conflicts of jurisdiction between Member States; adopting measures, establishing minimum rules relating to the constituting elements of criminal acts and penalties in the field of organised crime).

Therefore, the Council has the competence to deal with the above mentioned legal problems in joint actions (or, after the ratification of the Amsterdam Treaty, in frame work decisions) and in conventions. Considering the time required for the ratification of conventions, we would recommend to use – at least as a first approach – the instruments of joint

actions or framework decisions. In order to suggest priority actions, we would especially recommend to deal with the following joint actions (or framework decisions):

- creating minimum rules of criminal law for fighting international computer crime especially in international computer networks, including the harmonisation of accepted standards for contents,
- recommending adequate coercive powers (including solutions for encrypted data) with respect to the investigations of computer crime in international computer networks,
- dealing specifically with transborder investigations in international computer networks (e.g. freezing operations),
- solving conflicts of jurisdictions arising from international computer networks (especially with respect to illegal contents which could fall under a multitude of jurisdictions).

Creating minimum rules for illegal activities and illegal contents should be the basis for all other activities since the international prosecution of computer crime will not be possible in a country in which the respective acts are not criminal. The definition of such a list of minimum rules can be based on the work already achieved, especially by the Council of Europe and the Council of the European Union. Simultaneously, the procedural law issues should be based on the work which is already accomplished and presently continued within the Council of Europe.

C. Conclusions and Recommendations

The analysis of international and supranational activities in chapter IV described that the European Community has already enacted directives with precise requirements for the harmonisation of the non-criminal provisions of data protection law and of intellectual property protection. The previous analysis of competences (chapter VI) shows, that the EU has further reaching powers for legal measures against computer crime both under the first and the third pillar: Directives under the first pillar should concentrate on non-criminal prohibitions and rules (which may include general requirements for adequate sanctions), whereas measures under the third pillar should harmonise the sanctions of criminal law and criminal procedural law. In order to reach the necessary harmonisation in all of the above analysed areas of computer-related law, the present study especially recommends the following priority actions:

1. *Legal measures under the first pillar* can be based on Article 100a of the Treaty on the European Union. They could primarily focus on:

a. The elaboration of a directive on the general (civil and criminal) responsibility of access and Internet service providers (which should be elaborated before more national laws will enact such regulations).

   Such a directive could be based on the following principles:

   - providers should be responsible in accordance with general laws for their *own content*, which they produce or which they make available for use,
   - providers should not be responsible for any *third-party content* which they make available for use on their servers unless they have knowledge of such content and are technically able and can reasonably be expected to prohibit the storage of such content,
   - providers should not be held responsible for any *third-party content* to which they *only provide access* (unless they contravene concrete and non-appealable blocking orders).

b. The consideration of a directive which could define illegal and harmful contents in computer networks, which could not only require Member States to create effective sanctions against these illegal and harmful contents but also prohibit Member States to restrict international data flow with respect to illegal and harmful contents not listed in the directive.

   Such a directive could ban especially child pornography, racism, xenophobia as well as other illegal or harmful contents.

c. The inclusion of a list of illegal acts to be prohibited and covered by adequate sanctions of national law in a future directive (e.g. on electronic commerce) in order to guarantee security and consumer protection in European computer networks.

   The lists of acts could be based on the "minimum list" of the Council of Europe considering the update requirements of the AIDP, and include hacking, espionage, sabotage, manipulations and forgery.

2. *Legal measures under the third pillar* can be based on the K-Articles of the Treaty on European Union. They should concentrate on joint actions (or, under the Amsterdam Treaty, framework decisions), in co-operation with the Council of Europe and the P8 group. However, the EU should constantly look for a closer co-operation within the European Union than is possible within the framework of the other international organisations. The joint actions or framework decisions could be adopted with respect to

a. creating minimum rules for criminal law provisions with respect to international computer crime (based on the prohibition mentioned supra 1),

b. recommending adequate coercive powers with respect to the investigation of computer crime in international computer networks (balancing the requirements for effective prosecution and for human rights of suspects and witnesses),

c. fostering transborder investigations in international computer networks (especially transborder "online" investigations and freezing operations),

d. defining the range of national jurisdictions in international computer networks (especially solving conflicts of jurisdiction arising in international computer networks, e.g., with respect to illegal contents which could fall under a multitude of jurisdictions),

e. creating a set of common rules for a harmonised record-keeping in police and judicial statistics as well as for statistical analysis in specific fields of (computer) crime.

In order to avoid overlapping work by various international and supranational organisations, the European Commission could organise a joint conference or a workshop of the major players in the fight against computer crime (next to the EU, especially the Council of Europe, the P8, the OECD, Interpol and the UN) with the aim of bringing together and co-ordinating the work of these organisations. The analysis of this report could be the starting point for this co-ordinations effort. During or after this conference, it should be decided whether the EU will develop the instruments proposed above more on its own or more in co-operation (or by reference to) the proposals of other international bodies. In any case, mechanisms should be installed so that the results of the other international bodies can be incorporated in the solutions of the European Union. The aim of international actions should not only be to reach European, but also world-wide accepted solutions. The reasons for a Europe-wide harmonisation apply *mutatis mutandis* also for global solutions. Nevertheless, when monitoring and developing international solutions in other international bodies, it should be kept in mind that the European Union can come to a closer and faster harmonisation than e.g. proposals within the Council of Europe, the P8 or the United Nations.