ISBN 92-871-1792-6

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

LEGAL AFFAIRS

COMPUTER-RELATED CRIME

prefaced by August Bequai

European Committee on Crime Problems

Strasbourg 1990

COMPUTER-RELATED CRIME

Recommendation No. R (89) 9
on computer-related crime
and
final report
of the European Committee
on Crime Problems

Strasbourg 1990

French edition:
La criminalité informatique (Recommandation n° R (89) 9)
ISBN 92-871-1791-8

Strasbourg, Council of Europe, Publishing and Documentation Service
ISBN 92-871-1792-6

Printed in the Federal Republic of Germany

PREFACE

The computer revolution has had — and continues to have — a profound impact on the social, political and financial institutions of almost every nation in the world. Electronic Funds Transfer systems now handle much of the world's international financial transactions and the personal computer has become a permanent fixture of the modern office. Plans are also afoot to develop living computer chips that can be implanted in the human brain to replace damaged cells. Ours is truly a brave new world.

But the computer revolution has also spawned new forms of abuses and crime. Hackers now traverse our global computer networks at will and with impunity; techno-ethics are virtually non-existent; and modern criminals exploit the loopholes in our existing legal system to evade prosecution. The computer may well become the Achilles' heel of the post-industrial society.

Historians remind us that the future is a direct outgrowth of the past. Unless we learn from the past, we are tragically committed to repeating it — and the future is fast taking shape. Based on present-day trends, here is what we can expect:

— If international political turmoil continues unabated, global computer networks and telecommunication systems are sure to attract the ire of terrorists and the disfranchised.

— Tomorrow's wars will be won or lost in our computer centres, rather than on the battlefields. The destruction of a modern nation's computer systems could throw it into the Dark Ages!

— In Orwell's *1984*, the citizens of Oceania lived under the watchful eye of Big Brother and his secret police. In today's world, we all stand under the watchful eye of our giant computer systems. In the West, all that stands between us and Big Brother is the delicate political fibre we call democracy; if it were to collapse, the electronic edifice for a dictatorial take-over is already in place.

– The computer revolution has given a small group of technocrats a monopoly over the flow of global information. In the information society, power and wealth are increasingly becoming synonymous with control over our data banks. We live in the dawn of the informational élite.

The computer revolution has provided tools with which to steal with impunity, control and manipulate the thoughts and movements of millions, and hold an entire society hostage. On the other hand, if properly employed, the computer could dramatically improve the lives of billions on this planet. The choice is ours. Humanity's future need not be one of computer crime and terror.

For all these reasons, it is important that governments take the necessary steps to agree on a coherent attitude towards computer criminals. The Council of Europe report constitutes an essential contribution to that fight. It is warmly recommended for further study.

August Bequai, Esq.
Washington, DC
April 1990

CONTENTS

RECOMMENDATION No. R (89) 9

OF THE COMMITTEE OF MINISTERS TO MEMBER STATES ON COMPUTER-RELATED CRIME

(Adopted by the Committee of Ministers on 13 September 1989 at the 428th meeting of the Ministers' Deputies)

The Committee of Ministers, under the terms of Article 15.*b* of the Statute of the Council of Europe,

Considering that the aim of the Council of Europe is to achieve a greater unity between its members;

Recognising the importance of an adequate and quick response to the new challenge of computer-related crime;

Considering that computer-related crime often has a transfrontier character;

Aware of the resulting need for further harmonisation of the law and practice, and for improving international legal co-operation,

Recommends the governments of member states to:

1. Take into account, when reviewing their legislation or initiating new legislation, the report on computer-related crime elaborated by the European Committee on Crime Problems, and in particular the guidelines for the national legislatures;

2. Report to the Secretary General of the Council of Europe during 1993 on any developments in their legislation, judicial practice and experiences of international legal co-operation in respect of computer-related crime.

REPORT BY THE EUROPEAN COMMITTEE ON CRIME PROBLEMS

I. General questions

1. *Introduction*

a. *The work of the select committee*

The question of computer-related crime was included in the European Committee on Crime Problems (CDPC) work programme for 1985-86. The CDPC set up an expert committee to study the matter. The Select Committee of Experts on Computer-related Crime (PC-R-CC was the abbreviation for this committee; the members of the committee are enumerated in Appendix III of this report) began its work in 1985 and finished in March 1989. At the last meeting, the committee adopted the report and a draft recommendation which were transmitted to the CDPC for its approval. The draft recommendation and the report were approved by the CDPC in June 1989 and adopted by the Committee of Ministers of the Council of Europe on 13 September 1989.

The committee based its work on answers to a questionnaire as well as a report made by OECD (see OECD report, ICCP No. 10, Computer-related Crime: Analysis of Legal Policy, 1986, hereinafter referred to as the OECD report). It drafted guidelines for national legislatures in the light of reports submitted by the experts and the scientific consultants. The result of this work can be found in Chapter II of this report, which contains a detailed analysis of various forms of computer-related crime, including a description of the phenomenological background, the protected legal interests and a detailed commentary on the constituent elements of each offence.

Chapter III discusses procedural law problems with regard to the use of computerised data in criminal investigations. This chapter treats a problem which until now has seldom been discussed in a comparative perspective.

The committee has also discussed at length the transfrontier character of certain computer-related crimes and ways and means to fight such types of international crime. The committee considers, in Chapter IV of the report, the applicability of the European penal law conventions in this respect and makes certain recommendations and suggestions for future work, including the possible elaboration of a convention with the aim of harmonising substantive penal law.

The committee has also studied certain other important aspects of computer-related crime, such as the importance of security and prevention measures and the position of the victim of a computer-related crime. These aspects, together with certain general principles concerning computer-related infringements of privacy, are found in Chapter V of the report. With respect to the infringements of privacy, the committee has found it appropriate to recommend that further studies be undertaken by the Council of Europe in this field.

b. *Previous work*

The previously mentioned OECD report, prepared on the basis of a questionnaire-survey in OECD member states, contains the main lines of legislative policy in response to computer-related crime, an overview of the application of traditional criminal law and the development of computer-specific legislation, an analysis of the specific and unique aspects of computer-related crime and of substantive penal law as well as of certain international aspects of computer-related crime. It contains suggestions for the adoption of a common legal policy in the member states of OECD. In this respect, it was recommended that the OECD member states consider the following list of acts which could constitute a common denominator between the different approaches:

— 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;

— The input, alteration, erasure and/or suppression of computer data and/or computer programs made wilfully with the intent to commit a forgery;

— 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 telecommunications system;

— The infringement of the exclusive right of the owner of a protected computer program with the intent to exploit the program commercially and put it on the market;

— The access to or interception of a computer and/or telecommunication system made knowingly and without the authorisation of the person responsible for the system, either i. by infringement of security measures or ii. for other dishonest or harmful intentions.

As can be seen from Appendix I of the present report, the PC-R-CC has further developed and made precisions to the OECD list of offences, taking into account the work already carried out by OECD.

The Commission of the European Communities published, in June 1984, a survey on the vulnerability of the information-conscious society — European situation, summarised conclusions, which included a study of some 260 cases of computer incidents. Computer crime is one of the priority legal issues identified in the plan of action for setting up an information services market of the Commission of the European Communities (Council decision of 26 July 1988, *O.J.*, No. C 288 of 21 October 1988). At a meeting of the Legal Advisory Board of the Commission on this issue in May 1988, one of the experts' conclusions was that the Commission of the European Communities should seek ways to promote the application by all Community member states of the guidelines for the national legislatures (see Chapter II of this report) and other proposals arrived at in the Council of Europe. Recently, the Commission co-funded a series of seven projects, involving over forty organisations, in the area of security and protection of data, the protection of computer programs and the vulnerability of the information market. A brief report, entitled "The Legal Aspects of Computer Crime and Security", was also prepared for the Legal Advisory Board in 1988.

The question of computer-related crime was discussed within the framework of the Council of Europe for the first time by the 12th Conference of Directors of Criminological Research Institutes 1976 (see report by Professor K. Tiedemann in *Collected Studies in Criminological Research*, Volume XV, p. 26 *et seq.*).

Following this conference, the Select Committee on Economic Crime studied economic crime in general and drafted Recommendation No. R (81) 12 on economic crime. This recommendation was adopted by the Committee of Ministers in June 1981. It defines economic crime offences by enumeration. Computer crime (for example, theft of data, violation of

secrets, manipulation of computerised data) is considered as a "non-specific offence" which, in the context of the recommendation on economic crime, is to be taken into consideration only when it:

i. causes or risks causing substantial loss;

ii. presupposes special business knowledge on the part of the offenders; and

iii. is committed by businessmen in the exercise of their profession or functions.

As can be seen from the guidelines in Appendix I, the scope of application of computer-related offences, as the term is used by the PC-R-CC, is wider than that of the Select Committee of Experts on Economic Crime.

Finally, it is worth noting that the International Chamber of Commerce (Document 373/76, rev., published in July 1988) gives an international business view on computer-related crime and criminal law. This report is hereinafter referred to as the ICC report. The committee has also studied closely reports by several national commissions and their conclusions, for example the so-called Franken report in the Netherlands, hereinafter referred to as the Dutch report, the report No. 106 of the Scottish Law Commission (the Scottish report), a consultative memorandum by the same commission (the Scottish memorandum) and the working paper No. 110 of the English Law Commission (the English report). A select bibliography is given in Appendix II of the report.

c. *The phenomenology of computer-related crime*

The concept of computer-related crime

Information technology today constitutes an almost integral part of daily life. Computers have become an indispensable and pervasive tool in industrialised countries. Their influence on the content, form, time and space of daily activities, on the development of science and industry, on the functioning of organisations and on communication systems has transmuted modern living.

The new technology has brought a great many benefits to government and business administration and to the citizen himself. Its positive impact should not only be measured in terms of time and money alone. The computer has a liberating influence, too, by taking over, for instance, the repetitive and uncreative jobs that may make working life uninteresting.

At the same time, such a fundamental and rapid evolution raises a series of problems which may be socio-economic (for example with respect to fears of job losses) or legal in nature (for example as regards software ownership). The same applies to the crime control sector: the computer today offers some highly sophisticated opportunities for law-breaking. It can also be used to commit (or simplify the commission of) classical crimes, such as theft or fraud.

It may initially be noted that the committee, throughout this study, uses the term "computer-related crime" or "computer crime". No definition is generally accepted or recognised for these terms. The aforementioned group of experts that met within the framework of OECD adopted the following definition as a working definition: "Computer abuse is considered as any illegal, unethical or unauthorised behaviour relating to the automatic processing and the transmission of data." The expert group did not find it useful to aim at a more precise definition but chose instead a functional classification.

Writers have tried to define computer crime in various ways for the purposes of their studies of the subject. For instance, one expert has defined computer crime as "any illegal action in which a computer is a tool or object of the crime; in other words, any crime, the means or purpose of which is to influence the function of a computer". Another expert has defined computer abuse as "any incident associated with computer technology in which a victim suffered or could have suffered loss and a perpetrator, by intention, made or could have made a gain."

In the opinion of the committee, all attempts at defining the term computer crime have certain disadvantages that are not easy to reconcile with the aim of being succinct and precise and leaving no doubt as to the scope or the use of the definition. The definition by the OECD experts has a disadvantage in that it also includes unethical and unauthorised behaviour, even such behaviour that may not be a criminal offence, however reproachable it may be. The first of the above-quoted definitions suffers the weakness that the latter part of it seems to exclude unauthorised use of computers, whereas the first part of the definition may include several traditional offences which are not necessarily computer-related offences in the narrower sense.

These and other deliberations have led the committee to adopt the same, functional approach as the OECD expert group, without however the committee trying to give its own definition of computer-related crime. The notion of computer-related crime involves a variety of different types

of offences, some already criminalised by the various member states, others perhaps not yet dealt with sufficiently. By the drafting of the guidelines for national legislatures, it does not seem necessary to adopt a formal definition of computer-related crime which may create more difficulties than it solves. Computer-related crime is, as the term is used by the committee, simply then reduced to the offences enumerated and defined in the guidelines for national legislatures, which will leave it open for the various states to adapt this "definition" to their own legal systems and historical traditions, taking into account the offences on the minimum and the optional lists. This formal, and thus limited, approach means that certain types of computer-related crime, such as the trading in passwords, have been excluded from the work of the committee. A further explanation of the meaning of the guidelines and the division into a minimum list and an optional list is found in the beginning of Chapter II.

Amount of crime and losses involved

Opinions on the extent of computer crime differ widely. Media reports on spectacular cases and estimates of undetected ones suggest a large amount of offences with high financial losses.

A classic example of a computer-assisted economic crime is the Equity Funding case, in which the directors of an insurance company stored in a computer 56 000 fake life insurance policies with a sales value of $30 million and were found, when the accounts were closed, to represent two-thirds of the exchange value of the company's portfolio.

This case has become an example of a computer-related crime since the perpetration of the crime was greatly facilitated by the use of the data-processing system of the company. The individual insurance contracts were stored in the master file of the data-processing system. The reinsurer was willing to accept the computer print-out from the Equity Funding Corporation as evidence of the existence of the insurance contracts. The offenders simply added the data of the fictitious insurance contract to the data in the master file. To achieve this, magnetic tapes were used containing the data of old contracts already issued. A specially written computer program was used to change the old insurance numbers and multiply both the premiums and insurance sums to be paid by a factor of 1,8. Further computer programs ensured that the fictitious data were entered into the company's balance sheet.

As an example of input manipulation, one can cite the German case of the bank employee who transferred 1,3 million DM to her friend's account by simply crediting the amount in her own terminal, or the case

where an American student succeeded in linking a private terminal in his apartment via the public telephone network to the Pacific Telephone Corporation's central computer. He thereby authorised the delivery, free of charge, of goods worth about $1 million.

Such sensational cases cannot hide the fact that, according to reliable empirical studies, the number of verifiable computer crimes — apart from cases of illegal program copying and the misuse of automatic cash dispensers — is not very high (but the dark figure might be very high, see p. 17). Sufficient evidence of its presence can be obtained from official statistics, empirical studies and computer crime surveys.

The American Bar Association has completed a survey of some 300 corporations and government agencies, in which 72 of the respondents stated that they had been victims of computer-related crime within the last twelve months, their estimated annual losses ranging from $145 million to $730 million.

In a survey in 1981 conducted by the Local Government Audit Commission in the United Kingdom, 21% of the 320 firms covered stated that they had been victims of computer fraud in the course of the past five years. The 1984 survey resulted in 77 reported cases of computer fraud (943 replies, 55% response rate). In the 1987 survey, approximately one in ten of the 1 200 private and public sector organisations surveyed admitted to suffering fraud. The average admitted loss per case in 1987 was found to be about £47 000, with three cases running to more than £100 000. A conservative estimate of yearly losses in the United Kingdom from computer fraud, excluding damages caused by lost or disclosed data, is £30 000 000. Other estimates reveal much higher yearly figures.

During the 1988 *Sécuricom* Conference, the figure of 3,2 thousand million FF was advanced by the insurance companies as the annual loss resulting from computer incidents. According to figures advanced by APSAIRD in France (*Assemblée plénière des sociétés d'assurance contre l'incendie et les risques divers*), 31 000 computer-related incidents occurred in 1987 in France. 20 000 of these incidents were classified as "human errors", 9 500 were classified as "accidents" and only 1 500 were classified as "intentional incidents". However, this last category represented an estimated loss of 3,9 thousand million FF (+18% in comparison with 1986).

It is true that these figures need to be treated with caution as the differences between them are so great. Several of the aforementioned computer crime studies have also been criticised for being unreliable or exaggerated. For example, the study made by the American Bar Association had only a response rate of 28% (283 out of 1 000 questionnaires were completed and returned). As only 72 of the respondents reported a "known and verifiable loss due to computer crime during the last twelve months", the significance of the study was clearly weakened. The reported annual losses were only estimates and, as such, liable to mistakes by the person who had reported the figure.

It is the view of the committee that all figures regarding computer-related crime need to be treated with caution. However, the committee is also of the view that computer-related crime really exists and that it is a phenomenon that needs to be taken seriously by legislators. There is no need to report estimates when other, more reliable, figures show that the extent of verified computer-related crime is in itself cause to take it seriously.

Several examples of studies or official statistics concerning computer-related crime in the Council of Europe member states could be quoted. Criminal statistics from the Federal Republic of Germany show that 3 067 cases of computer crime were reported to the police during 1987. 2 777 of these cases were considered by the police to be a case of computer fraud under Article 263.*a* of the Penal Code (most cases probably concerning automatic cash dispensers). These police-registered cases led, in 1987, to 150 convictions. 169 cases (17 convictions during 1987) concerned falsification of data, 72 cases (eight convictions during 1987) were considered to be cases of data alteration and sabotage and 49 cases (one conviction during 1987) of data espionage were reported. It is noteworthy that these official statistics do not cover cases of illegal copying of computer programs. It is also interesting to note that there were 1 112 suspected offenders of the 3 067 police-registered cases and that 71% of the suspects were over 21 years of age. Since the enactment of the new French Act of 5 January 1988, eight cases have been brought before the courts during 1988.

All verified serious embezzlement offences in Sweden, 1981-83, were analysed by a criminological researcher. Of the 351 cases, 38 included computer-related embezzlements. The Austrian Ministry of the Interior, to whom all security agencies have to report cases of computer crime, registered 30 relevant cases until the end of 1985. The previously mentioned EEC report (see page 11) revealed some 260 computer incidents in several countries.

The extent of losses is a much disputed area, too. Investigations in the Federal Republic of Germany some ten years ago indicated losses from computer manipulation of between 200 000 and 300 000 DM, which in some cases were even higher in the following years. In Sweden the above-mentioned study revealed an average amount of 196 000 SEK for computer-related embezzlement. A private study from 1984 in the United Kingdom found average losses of around £31 000 in the field of computer fraud. These and other studies suggest that losses, at least from computer manipulations, are on average higher than traditional kinds of fraud.

While it is possible to give a general idea of the diversification of computer crime, it is virtually impossible to supply full, accurate quantitative data concerning the number of cases and the amount of losses (see the Scottish report). Estimates in the United States of the dark figure (99%, 95% or 85%) and yearly damages up to between $100 and $300 million, $145 and $730 million (see the OECD report), or even $2 thousand million have been criticised not only in the United States, but also in Europe (see the Scottish memorandum).

Despite such controversies, it is generally assumed that the number of undiscovered computer offences is considerably higher. Difficulties of detection and evidence, together with a lack of knowledge on the part of investigating authorities in the complex data processing and telecommunications sector, are one reason. Another, and maybe more important one, is the reluctance of victims (for example banks, insurance companies) to report incidents or divulge any related information (see Chapter V of this report) due mainly to a fear of losing goodwill through adverse publicity and of loss of confidence by investors, shareholders and customers. In addition, this attitude may facilitate the settlement of damage claims between victim and offender.

The conclusion may therefore be drawn that computer-related crime is a real and, at least in respect of certain offences, expanding phenomenon, even though some of the more deliberately sensational statistics are probably not reliable. Furthermore, a steady increase in the number of cases must be expected, if only because of the ever-larger numbers of computers installed, not least home computers. The time has clearly come for every industrialised country to put in hand a series of preventive measures in the field of security or of instruction in computer ethics, and to respond to this form of crime with appropriate legislation.

Environment, types and specific features of computer-related crime

In this form of crime which Bequai regarded as "part of a larger form of criminal activity: white collar crime", a number of factors have a specific role.

The particular environment in which the instrument functions is not without relevance. The concentration of easily changeable information in computerised and interconnected systems can make it more vulnerable as regards its availability, integrity and exclusivity (see the Dutch report). A data bank generally contains a sizeable volume of information, seen more and more as an economic asset. A company can put its own future at risk by storing sensitive or strategic information concerning the development of new products, details of finance, or lists of customers. Computerised information is therefore becoming an item of property, over which it is now increasingly common for industry to claim exclusive rights in relation to third parties.

The physical location where the information is collected and stored necessarily becomes a vulnerable spot which the owner of that information must guard. The computer centre, the terminals, lines of communication and all data carriers constitute easy targets for malicious acts and so warrant specific preventive measures. This problem assumes an additional dimension when data are transmitted from one computer to another (network insecurity) or are passed across frontiers.

Equally specific are the *modi operandi*, designed for the automatic routines in the computer system. Here, the existence of a special, highly imaginative jargon does nothing to make a lawyer's intervention any easier. Terms such as "salami technique", "Trojan horse", "superzapping", "piggy-backing", "logic bombs", "computer virus" and "data diddling" keep the uninitiated in a state of bewilderment.

A further aspect of the intangible nature of information is the much more casual attitude that prevails in the sector where operations are monitored. Insufficient security measures may create new possibilities of harming interests of the state, of the business community and of private citizens. When information is stored in a computer, the technical process is, according to certain experts, subjected to only a tenth of the number of controls that would be applied to the same information handled manually. It all takes place not in a matter of hours or of minutes, but in a matter of milliseconds. This reduces the chances of being caught. It is claimed that, on average, an illegal activity in this sector can continue undetected for several years. Spatially, telecommunications and information networks have eliminated the distance factor. It is probable, therefore, that many cases of computer crime transcend national frontiers. The activities of the children of Dalton School in the State of New York who infiltrated about twenty Canadian data banks, including the files of public authorities, are an illustration of this. Another is the violation of the NATO system in Norway from the United States, the breaking into the NASA worldwide data network or into a computer in the Higher Energy Institute in Tsukuba, Japan (the "Tristan case"), and the espionage case revealed in February 1989, all three last-mentioned incidents concerning the Federal Republic of Germany. Other transborder cases concerning "viruses" (a "virus" is a small computer program which can often reproduce itself and infect other computer programs, thereby causing damage, deleting data, hinder the functioning of the program, etc.) are reported, for example the "Israel virus" and the "Pakistan virus".

It is also very interesting to see what type of people are involved. The media and some experts divide known cases into intrusions by accidental and really criminal offenders. The former are usually attributed to young computer-mad whizz-kids or "war game" enthusiasts who enjoy a challenge and have learned all the tricks, including how to break into security codes and keys ("short-pants crime"). Publicising such hacking acts may be useful in some instances as regards the detection of loopholes in computer systems. However, in general, they are considered to be dangerous. Data may be destroyed by negligence, system blockades may be caused and security deficiencies may be misused subsequently (see the concern of the United States Congress when passing the Federal Computer Fraud and Abuse Act of 1986). It is often asserted that more serious crimes, entailing high financial damage, are committed by technically accomplished persons with a university background or advanced technical training, sometimes even with experience of code-breaking. Criminological research — in the Federal Republic of Germany for example — has only partly confirmed this assumption. Many offenders are their victims' employees with good knowledge of the firm's organisation. Accustomed to mobility, they may not particularly identify with the companies for which they work and may therefore, in some instances, not spontaneously consider it criminal to attack the "system". But usually their motive is gain-oriented, sometimes determined by need. Acts of computer sabotage by employees are often acts of revenge. In other cases, a revolt against the "anti-social or inhuman machine", a sense of challenge, of competition, or the misuse of a privileged or exclusive élite position may be the cause.

2. *Criminal policy considerations*

a. *International development of computer-crime legislation*

In most of the member states of the Council of Europe, the new phenomenon of computer criminality has in the last ten years prompted an examination of whether the domestic criminal law provides a sufficient range of responses to the new kinds of abuse made possible by computer technology, or whether it needs adaptation, further development and supplementation. In the meantime, a number of member states have already introduced more or less extensive amendments to their substantive criminal law (Austria, Denmark, France, Federal Republic of Germany, Greece, Liechtenstein, Norway, Sweden), whereas others have made only isolated supplements (for example, Spain, Portugal and the United Kingdom). Outside the Council of Europe, it is particularly the new statutes in Australia, Canada, the German Democratic Republic and Japan and the numerous amendments to the law at federal and constituent state level in the United States which should be mentioned. Other states are either preparing corresponding statutes or thinking along these lines (for example, Finland, Italy, the Netherlands, Switzerland, Turkey and the United Kingdom).

The above-mentioned analysis of national criminal policy (see I.1.*b*) by an OECD working group indicates common areas which provided the basis for initial recommendations at international level. In all of the industrialised states, the same phenomena of computer crime have appeared; prosecuting authorities almost everywhere have to contend with similar difficulties in the application of the traditional domestic criminal law to this new form of crime; dramatic cross-border cases demonstrate the increased need for international co-operation. All this has led to a consideration of the possibility of moving beyond the domestic plane to develop joint strategies for the suppression of the new types of offence at international level. These relate to different, but interconnected, levels in the fight against crime:

— stipulating what acts constitute offences by possible amendments and supplements to the substantive criminal law;

— effective prosecution, *inter alia* by possibly adapting domestic criminal procedural law and related provisions;

— improving international collaboration.

The composition of the committee, with mainly lawyers specialised in criminal law, has meant it has looked only very generally at the development of preventive measures (see below, V.2), to which, in the committee's view, high priority should nevertheless be accorded.

b. *A European criminal policy*

At the centre of the committee's work stood the development of common guidelines for the national legislator with regard to the adaptation and further development of the substantive criminal law. As is well known, criminal law is among those fields of law which, at the European level, have thus far offered but few openings for harmonisation. The retention of national characteristics in scope and framing, and the weight of tradition lead to the special emphasising of national sovereignty in the formulation of criminal law policy objectives. The area of computer crime opens up the chance to develop, in one particular sphere, a European criminal policy which is also acceptable in the domestic arena. The committee here has set off along a cautious path.

For the time being it is confining itself to the development of what are termed "guidelines" and a recommendation to support these guidelines. If a study reveals that the level of harmonisation in respect of computer-related crime is inadequate, the committee proposes that the elaboration of an international convention should be considered (see Chapter IV of this report).

The guidelines are to be found in Chapter II. The thoughts in them on the criminalisation of certain dangerous modes of behaviour are to be seen in relation to the following general reflections on criminal policy.

c. *Legal interests protected*

Legal policy decisions, which regard the use of the criminal law as one of the most incisive means of social control by the state, presuppose, first of all, a specification of the social or individual interests which are impinged or endangered by certain modes of human behaviour in the handling of new technology. The reactions of those affected, criminal proceedings and empirical investigations show that attacks on hardware, software, data and computer systems, or the abuse of these components, can produce results which are considered not only as undesirable, but as harmful or at least dangerous. Just as it is difficult for the phenomenon of computer crime to be encapsulated in one precise, general definition, so it is hard to make a uniform pronouncement on the dangerousness of

particular manifestations of computer crime. Closer specification of the legal interest (in German *Rechtsgut*) threatened by various possible forms of abuse, and also of the degree and potency of the dangers, must therefore be among the necessary initial considerations if we wish to avoid over-criminalisation.

i. On the one hand, we can see that data processing and its components are frequently only used as a tool in the committing of what in themselves already constitute offences. In such cases these tools can, it is true, lend the offence a new dimension (perhaps it could not have been committed at all using traditional means, as the Equity Funding case shows, see Chapter I.1); in reality, however, they only represent a new *modus operandi*. The spread of data processing to all parts of life today makes it possible, in the final analysis, to jeopardise all interests worthy of protection by abusing the new technology. Examples are manipulations (or even only supervisory errors) in a computer-controlled surveillance system in the intensive care unit of a hospital which result in the death of a patient; microprocessors in motor vehicles or aircraft can become the object of acts of sabotage. Further examples are tax evasion, falsification of balance sheets, capital investment fraud, stock exchange manipulations, the endangering of national security interests, the breach of trade secrets or of a person's private sphere. In so far as a legal interest enjoys sufficient criminal law protection against violation or endangerment, no further problem arises as regards the criminal law assessment of EDP-related acts.

The computer dimension, as such, should not be viewed as an aggravating circumstance. As a result, the increasing abuse of EDP, leading to an impairment of classical legal interests, might mean that the totality of criminal legislation will have to be reconsidered with computerised activities in mind. In this respect, however, the committee has imposed restraints upon itself. It has included in its considerations only those acts which have thus far been most significant in practical terms (in this respect the Dutch report covers more offences than discussed here). Legal gaps have resulted in particular from the following:

The criminal law is often characterised by the fact that it offers only fragmentary protection for certain legal interests. In many cases, criminal law protection has only extended until the present to physical, tangible and visible objects. Further extension might founder on the *nullum crimen sine lege* principle together with the criminal law ban on analogous application of statutory provisions. The offence of fraud may protect property interests only against practices consisting in the deception of a person, not against so-called computer manipulations. The traditional offence of forgery may require that statements constructed with corporal objects are forged, which rules out the inclusion of changes of stored data. This shows that certain legal interests are not protected against new forms of interference made possible by the use of EDP. Whether legal interests should be protected against new kinds of attacks is something which none the less requires further assessment (see under *d*). The prerequisite here is in any case a comparison of the interests prejudiced in the computer and non-computer area (see the Guide for legislators and policy advisers presented by Mr Piragoff at a symposium on computer crime, held at the *Vrije Universiteit*, Amsterdam, 22 April 1986, the Dutch report). This may show that the computer variety may typically be even more dangerous than a traditional mode of commission (see the higher amount of financial loss caused on average by computer fraud compared with traditional fraud, *supra* I.1.*c*). On the other hand, it is also possible that some computer-related offences occur much more rarely than traditional ones (as is partly presumed, for example, in respect of the falsification of stored data which are relevant in evidence).

ii. In some instances, however, computerisation has led to situations where new types of interests are emerging which call for legal protection. It is possible that the correctness of the information or the reliability in the functioning of a computer system could be considered as legal interests in themselves worthy of criminal law protection. The various manifestations of computer criminality include new forms of violation of objects possibly worthy of such protection. This is particularly the case where the targets of such acts are stored or transmitted data or computer systems. Even there, it has been argued, the said interests are not really new in a qualitative sense but rather derived from the traditional set of values. Interrelationships become visible, for example, in the structuring of possibly violated interests in the Dutch report in the distinction between:

— the availability of the means of storage, processing and transfer of data and of the data themselves;

— the integrity of computer systems and the data they contain;

— the exclusivity of certain data.

Examples are the unauthorised erasure or alteration of stored data, interfering with the functioning of computer systems or the unauthorised acquisition, disclosure or use of stored data. This shows that computer crime involves new interests in some areas. The classic offence of criminal damage protects only tangible things against damage to substance

and function and alterations to their outward appearance. Cases of data espionage show in a comparison with espionage cases in the non-computer area that data are indeed protected in certain respects by current law (for example, by patent, copyright, unfair competition, privacy law) against unauthorised acquisition etc. In these areas we see the emerging role of information and intangible values, leading to difficult demarcation questions between what is and what is not worthy of protection. Particularly with the aid of the computer, valuable knowledge can be stored in the smallest of spaces with enhanced availability. This can also result, however, in enhanced possibilities of damage. In our societies built on the free flow of information, information generally should not be accorded absolute and exclusive protection in the sense of a property right (see the OECD report, p. 42; the Dutch report, under III.1). In the light of the specific type of information at stake and the security measures involved, a concrete assessment of conflicting interests has to be made in order to determine to what extent a specific type of information is worthy of protection. The interest of the creator or holder of information, who has invested labour, money and time in research and development, in preserving and exploiting the results of his efforts has to be balanced against, for example, the interest of society in the unrestricted spread of new knowledge.

d. *The principle of subsidiarity*

That certain interests are singled out as generally deserving protection against interference arising out of the use of computer technology does not automatically mean that criminal law protection should be granted or that it is necessary to enact new criminal law provisions. Criminal law should only be resorted to as a final step, if other means of dealing with problem areas are insufficient (principle of subsidiarity). Criminal law should be, on the one hand, subsidiary to non-legal measures, on the other hand, to civil, commercial and administrative law. Particularly because this principle is often ignored in practice, the committee considers it appropriate to give a reminder of this point, too. In this it is also following the line of Recommendation No. R (81) 12 of the Committee of Ministers to member states on economic crime, which also relates to certain cases of computer crime.

One of the most effective means of preventing computer-related crime is the development and introduction of security measures, an approach which, when combined with efforts to increase awareness of the possibilities of abuse, is also regarded even by criminal law experts as being fundamentally more important and holding out greater prospects of

success than enhanced criminal law protection. However, due to constant technical progress and human failures in the application of security measures, even comprehensive technical, organisational or personnel-oriented safeguards are unable to provide absolute protection, or at least a level of protection so high as to consider negligible the few remaining abuses. In addition, in order not to produce negative or counter effects for the effectiveness of computer systems, the density of such measures, the costs and the efforts they require, have to stand in some sort of reasonable relationship to the protective effect sought, considerations followed not only by the data-processing department of an enterprise, but also by auditors and insurance companies demanding a certain level of security measures.

There is no doubt that other legal measures, too, can have a preventive effect, such as compensation claims or administrative law measures. This particularly applies where the above-mentioned security measures are given a statutory basis, as has been done using a flexible approach in part in some of the data protection acts of the member states. Other examples are compulsory examinations by auditors (combined with the development of a self-regulating code of conduct for that profession), or the possible introduction of an obligation on the part of enterprises to provide, in their annual accounts, information on the reliability of the data processing (see the Dutch report). According to their function, these measures may be limited in their effect. Compensation claims fail if the person who caused the damage has insufficient means to satisfy the claim or where the real damage cannot be measured in terms of money. The sanctions following a violation of administrative law may be too limited for the purpose of prevention and repression. Codes of conduct are only applicable to members of professional organisations.

All these examples show that this subsidiarity has its limits in the area of computer-related criminality. Obviously, confining the criminal law to a subsidiary role in this field does not therefore imply not using it or even abolishing it. In their efforts to deal with prevention, control and supervision of asocial acts directed against or perpetrated by means of computers, states should not overlook any of the resources at their disposal. A combined effort to contain and reduce (possible) computer-related offences by a balanced variety of means is necessary, in which criminal law provisions and their enforcement play an important role. If some measures or institutions prove inadequate, it is justifiable to resort either to amending current law, including the criminal law, to reinforce its impact and effectiveness, or to creating new institutions and even new offences. Subsidiarity of the criminal law in this field means, while empha-

sising and maintaining the role of civil and administrative law, to concentrate and restrict the criminal law to a hard core of offences where these branches of the law are not sufficient to prevent computer crime and there is clearly an abuse of computer operations showing manifest criminal intent. This reinforces the deterrent, that is the preventive and repressive effect and the importance of criminal law and of the criminal justice system.

The concept of subsidiarity also shows itself in the relationship between the existing criminal law and the prospective new ones. Before having recourse to legislative remedies, every effort should therefore be made to apply current law to new forms of crime as far as possible in order to avoid over-criminalisation and the overlapping of criminal law provisions. In the actual practice of prosecution, this has also largely been the rule up to now. A detailed treatment of the application of traditional crimes such as theft, fraud, breach of trust, forgery of documents, the copyright criminal law or, for example, of criminal law provisions against the violation of trade secrets, is contained in the OECD report (pp. 29-65). A new example is the decision by the Swiss Supreme Court (18 December 1985), applying the provision on forgery to the falsification of electronic impulses. Only where no such provision is applicable, due to a lack of one or more of its essential elements, should the amending or creating of criminal law provisions be considered. Acquittals due to the absence of an appropriate offence category are the exception (for example, the decision of the Supreme Court of Canada, R. v. Laughlin (1980), SCR 331). How large the gaps really are, quantitively speaking, is something which certainly cannot be stated with accuracy, however. Considerable uncertainty exists as to the dimensions of computer crime. Apart from the unauthorised copying of computer programs and instances of abuse of automatic cash dispensers, the number of confirmed cases in the member states and abroad is not particularly high. The question of the frequency of occurrence of certain abuses is significant not only for criminology, but also for legal policy measures. If gaps in legislation are on the one hand clear, but such abuses occur only seldom, this may mean that the legislator, at least provisionally, will regard statutory amendments as not being necessary. A consideration of the available evidence about the scale and the seriousness of computer-related crime is therefore to be recommended. In view of difficulties with regard to detection, inadequate safety precautions and a widespread tendency not to report cases to the prosecuting authorities, criminologists deduce in general, however, the existence of a considerable number of cases which have not come to light. Under these circumstances it may be appropriate for the legislator to close gaps now in criminal law, at least for acts with serious consequences, rather than

wait for a thorough investigation of the number of undetected crimes. Given the level of damage which has been recorded at least for some computer abuses, it would, in addition, be a mistake only to take legislative action following a number of acquittals.

The application of the law currently in force has limits set to it by the analogy prohibition contained in the criminal law. Since, however, the boundaries between extensive interpretation and prohibited analogy are vague, the courts may still enjoy — where applicability to new kinds of cases may be doubtful — the possibility of stretching the criminal law. Such a road, however, does not offer unlimited access, and is also beset with dangers. An offence category should not be stretched too far as was sometimes the case, for example, with the application of the breach of trust offence to computer manipulations in the Federal Republic of Germany. The structure of the offence category, its actual classical scope, may in such cases undergo an unintended and undesired alteration and extension. The principle of making penal provisions clear and precise should prompt the legislator in such cases to opt for the course of creating supplementary or new provisions. This approach will also avoid the danger of over-criminalisation by the adoption of new legislation.

Prior to any decision in favour of legislative measures, the criterion of subsidiarity should also be heeded by examining whether it is not possible, via procedural law (see on this Chapter III, below) and practical measures, to enhance the applicability of existing law so that it sufficiently stems the flood of computer offences. In this sense, subsidiarity is related to the enforcement of existing law by an improvement in the organisation of the police and judiciary. The committee clearly supports all efforts to provide investigating and prosecuting authorities, as well as the courts, with the technical means necessary — plus the appropriate experts — for evidence to be obtained by adequate means, and with an efficient training of personnel at all levels (see Recommendation No. R (80) 3 of the Committee of Ministers concerning teaching, research and training in the field of "computers and law"). Such measures take on particular significance where problems occur with regard to evidence. They do not, however, produce effective prosecution where the difficulties lie in obvious gaps in legislation. Practical measures are therefore only to a limited extent a substitute for legislative measures, and have their primary effect in lending greater weight to the latter's enforcement.

e. *The possible scope of criminalisation*

A decision in favour of criminalising certain forms of computer abuse is thus dependent on the one hand on identifying a definite impairment

or endangering of interests worthy of protection, and also on what is said about the effectiveness of other measures (including the application of existing law). Over and above this, however, one should not forget an assessment of the effectiveness of new criminal law provisions either. As regards their general preventive effect, however, there is little that can be said. As deterrence is dependent on the offender's assessment of the likelihood of being caught, the speed of adjudication and the severity of punishment, the amendment of substantive criminal law has to be seen in the context of the functioning of the criminal justice system. It must be able to deal by proper means of enforcement with the new forms of crime. In this respect there is a relationship between substantive criminal law, criminal procedure law and the above-mentioned practical measures. Finally, there is a general need to weigh up the advantages and disadvantages of criminalisation (their so-called "social costs"); this is particularly true when it comes to establishing boundaries. And it is clear above all in relation to the question of how far data and information ought to enjoy criminal law protection. We should not lose sight of the danger of over-criminalisation. As with the identification of impaired interests and the general extent to which they merit protection, a comparison of parallel cases in the computer and non-computer area, with the visible scope there of traditional offence categories, provides a yardstick for the scope of criminalisation (see the Dutch report; Piragoff's guide, *supra*). All the same, this does not rule out decisions by the legislator to protect interests in the computer environment that are not protected in the non-computer environment (for example in respect of the alteration or addition of data). Such extensions, however, need to be particularly carefully thought out.

f. *The relationship to existing legislation*

In most member states, new legislation bears the imprint of a close link and direct reference to already existing penal provisions or legal policy considerations (see, on the last point, the Dutch report and the Scottish report). This is self-evident where the policy is to review existing legal concepts on which the present definitions of offences are based and to adapt them to new situations arising from computer technology. Various approaches are used. France has introduced a whole new chapter in its Penal Code. A similar approach is contemplated in Italy. In other countries, redefining or amending of existing definitions (for example "document" to include data stored on a data carrier, as in Canada, Greece, Finland and in the United Kingdom) has been considered sufficient to ensure that the traditional offences, like that of forgery, adequately apply. In other cases, the existing provisions have been supplemented by new criminal

acts and other constituent elements, which in some instances can be done just by adding a further subsection. Finally, in some states, completely new criminal law provisions have been created, following existing provisions, either in the form of an additional subsection (Greece, Norway, Canada; see the Dutch report) or quite independently (Austria, Federal Republic of Germany; see the Swiss draft). This method in particular is suited to combating the danger of over-criminalisation.

Independent regulations are especially to be found where new objects of legal protection play a role — for example, in the case of unauthorised entry to computer systems, unauthorised eavesdropping on a computer communication or unauthorised acquisition of stored data — although here, too, to a certain extent parallels with existing penal provisions (like wiretapping, violation of the secrecy of letters) can be drawn.

"These acts may be expressed as far as possible in terms of functions rather than technology" (OECD report, p. 69). The adaptation of the criminal law to the technological process does not mean that, for example, computer processes acquire the rank of essential elements of offences. Although preciseness is important in the wording, the offences should not be so technologically oriented that the new provision ceases to be effective in the near future when the same abuse is done by somewhat different means as a result of technological development. Therefore the offences should be framed in more general abstract terms, but be sufficiently precise and descriptive in order not to create uncertainties as to the limits of the offence and to enable computer users, with the support of professional regulations and codes of conduct, to adapt their behaviour.

The great differences between specific forms of computer abuse allow the legislator to proceed step by step via a number of separate pieces of legislation, without thereby running the risk of abandoning a coherent criminal policy. Thus up till now, for example, amendments of copyright law relating to cover for computer programs or the introduction of protection for topographies have always been passed in separate Acts, that is, independently of amendments to the Criminal Code. As these examples show, this is particularly appropriate where amendments of the criminal law are closely related to the necessary amendment of civil law, economic law and administrative law provisions. An example of the latter might be the amendment of penal provisions in data protection statutes. In many cases, it will then also be found that abuses which occur

in the use of computer technology are only examples — albeit spectacular ones — of a more extensive, more general problem. Such areas, however, including for example computer espionage and resulting in the violation of trade secrets, have also been included by the committee in its recommendations (although the Scottish report does not go this far). It has not, however, made a comprehensive examination of them, considering them instead only with specific reference to computers, and, in the sphere of data protection, it has even confined itself to general deliberations on (de-)criminalisation.

g. *Modulating criteria*

In framing amendments to the criminal law, the legislator will primarily remain within the framework provided by the traditional structures and legislative techniques of the domestic criminal law. None the less, the committee regards it as appropriate to stress the modulating criteria which may play a special role in the field of the criminal law as it relates specifically to computers.

i. Where, in framing the criminal law relating to computers, it is not only a question of creating provisions parallel to existing penal provisions, one might contemplate introducing, as an essential element, the causing of (substantial, significant) damage or injury. With this in mind, the footnote to the appendix to Recommendation No. R (81) 12 on economic crime includes computer crimes among economic crimes when they cause substantial loss. An example of this is an alternative approach to the offence category of unauthorised use of computers, below. In a great number of computer offences, however, it becomes evident that risk situations must also be included. This is also acknowledged in Recommendation No. R (81) 12, where among economic offences inclusion is also made of computer crimes which only risk causing substantial loss.

ii. Other alternatives in the footnote mentioned in sub-paragraph i prompt the consideration of penalising only those acts whose commission calls for particular knowledge in the computer field, that is creating offences which can only be committed by a certain category or type of person, in other words, making computer-related offences "special offences" (*Sonder Delikte*). These criteria, which in Recommendation No. R (81) 12 have arisen out of the endeavour to demarcate between economic and non-economic offences, appear problematic in the light of the general growth and spread of knowledge in the computer technology

field. They may result in the computer-related criminal law becoming too narrow in its application, as for example cases of what is termed "hacking" have shown.

iii. Another criterion relates to the distinction between offences committed within the computer system and those directed against the system by outsiders. This is the case in legal systems which adopt a notion of unlawful act (*acte illicite*), as opposed to acts without right (*acte sans droit*), encompassing breaches of contractual obligations such as employee-employer obligations. The exclusion of contractual relationships is indeed an alternative worthy of consideration, given the possible subsidiarity of the criminal law as against civil law rules on cancellation of contract and damages. It can be found for instance in statutory provisions or legal policy considerations in relation to limiting the penalisation of cheque card and credit card abuse to outsiders (for example in the United States; French *Cour de Cassation*, 24 November 1983). Assessments vary here from state to state (a differing assessment, and one in favour of more extensive criminal law protection, can be found for example in the Federal Republic of Germany).

iv. An objective criterion consists of making a distinction according to whether or not there are technical devices for the protection or security of computer systems, data banks, programs or data. To use such elements as a restrictive criterion serves the principle of subsidiarity, too, and may be an incentive for the owner of computers etc. to take all precautions necessary according to the circumstances and his personal situation. The legislator may, however, decide to go further and to punish even those offenders who misuse the situation of a victim who has failed in the protection of the computer and its different parts.

v. An important distinguishing criterion for the gravity of an offence is the form of guilt. Should not only acts committed intentionally, but also committed recklessly or even only negligently, be criminalised? Should the repression of intentional acts be modulated according to the motive or intention behind them? The options depend partly on what are considered to be the characteristics of legally protected interests. In so far as only property or economic interests are violated, then normally only intentional offences will be considered criminal (see the guidelines, *infra*). If the computer is used as a new tool to commit offences violating higher objects of legal protection, the assessment may be different.

On the other hand, there are also areas where thought must be given, even for intentional acts, to limiting criminal liability in the subjective domain still further. This might mean not accepting possible intent (*dolus*

eventualis) as sufficient, or requiring the existence of particular intentions (for example, enrichment intention, intent to damage another, etc.). In some cases, such criteria may also serve as constituent elements for more severe penalties (see the Swiss draft).

vi. Finally, another criterion could relate to procedural prerequisites for prosecution in some countries. There, a distinction must be made between countries which have established the principle of discretionary prosecution and those which adhere to the principle of mandatory prosecution. These two principles have been discussed in detail by the Select Committee of Experts on Simplified and Summary Procedures in Criminal Cases, see Recommendation No. R (87) 18 by the Committee of Ministers on the simplification of criminal justice.

The possibility of prosecution on the basis of a complaint exists not only in countries which adhere to the principle of mandatory prosecution but also in some countries which are governed by the principle of discretionary prosecution (for example in the Netherlands). It gives the opportunity to look for criteria to distinguish between these two types of prosecution, for example according to the extent of the injury, the seriousness of the offence, the form of guilt, whether the offender acted to obtain an unlawful gain or undue advantage (see the Swiss draft). If a complaint is necessary, the result may be that acts that are not very serious, having caused only a small or insignificant amount of harm, will not in principle be punished. Another means of modulation is the combination of the prerequisite of a complaint as a rule with the exception of mandatory prosecution if there exists a special public interest in this (the Scandinavian countries, Austria and the Federal Republic of Germany).

h. *The relationship to criminal procedural law*

Substantive criminal law can only be applied through the medium of criminal procedure. It ensures that this is done fairly. This is reached by a balancing of the interests of society in an efficient application of the substantive law in an endeavour to uncover the truth, and of the interests and rights of suspects who become an object of investigation. The use of computer technology has created not only new possibilities to commit new abuses, but has also produced new traces of evidence stored in computer systems or on data carriers. The use of these new sources of evidence causes in some instances not only practical difficulties (see the examples in *The International Handbook on Computer Crime*, by Sieber, p. 139 *et seq.*) but also legal problems. They relate, for instance, to the

application of the provisions on search and seizure to the access, recording and use of stored data, or those on wiretapping to the interception of telecommunications. The use of such materials in court proceedings might also lead to problems. The committee shares, in general, the opinion that adaptation of national law might be necessary in this field. National and international discussion has started only lately (see Sieber, *supra*, pp. 110 *et seq.*; the Dutch report; Kaspersen, in the *Legal Aspects of Computer Crime and Security*, document prepared for the Commission of the European Communities, Legal Advisory Board, 1987, p. 58 *et seq.*). It should be continued. Some observations and suggestions for future investigation and possible legislative action are included in Chapter III of the report.

II. Guidelines for national legislatures

1. *Introduction*

1. It has already been emphasised under I.2 that the difficulties of counteracting the new phenomenon of "computer crime" using traditional criminal law have actually opened up the possibility of developing a uniform criminal policy in this field. The guidelines for national legislatures serve this goal. The starting-point is the variety of specific acts, which give cause for closer examination of the question as to which individual or social interests are violated or jeopardised by computer-related offences. The committee has elaborated the guidelines having regard to the general criminal policy considerations referred to under I.2 and the legal development that has taken place in the various member states over the last years and also in states that are not members of the Council of Europe. The starting-point was provided by the investigations, conclusions and suggestions of OECD (see I.1). The committee has continued to develop guidelines that it expects to be taken into account by the member states when they are reviewing their legislation relating to computer crime.

2. The elaboration of a minimum list illustrates the consensus of the committee as regards the assessment of the special danger and harmfulness of a hard core of certain computer-related abuses that should be dealt with by the criminal law. The term "guideline" also constitutes, in this connection, an appeal to those responsible for the development of national criminal policy and its conversion into legal provisions to allow themselves to be guided by this European consensus. Correspondence in the coverage of national criminal law may prevent abuses from being shifted to and committed in those states whose criminal law previously

exhibited loopholes. It also facilitates international co-operation in suppressing the various manifestations of computer crime by way of mutual legal assistance and extradition (see Chapter IV of this report).

The minimum list constitutes a further development of the OECD list. It contains supplements; sharper distinctions have been drawn between individual types of offences. Against the background of new national legislation, the descriptions of offences have been improved. This list now covers the area of computer manipulation (computer-related fraud, computer forgery), interference with computers and data (damage to computer data and computer programs, computer sabotage), spying out (unauthorised access and interception) and cases of illegal copying of valuable computer-related objects (unauthorised reproduction of a protected computer program or of a topography). It must be noted that the descriptions of individual offences, as given in the guidelines, represent a minimum consensus as regards the desired criminal law coverage. Additional extensions against the background of national law are not ruled out.

3. The abuses put on the optional list are primarily of the kind that have already played a role in pratical terms and may increasingly do so in the future as well. However, as regards their inclusion in the field of computer crime or their criminal policy assessment, it was not possible to achieve the same degree of consensus as with the offences on the minimum list. The criminalisation of these abuses is nevertheless often advocated or regarded as worthy of consideration. To some extent there is only discussion on the desirable borderline for criminal liability. An expansion of the criminal law to include these areas is regarded by some as being too extensive, and other instruments for averting harm and danger are considered sufficient.

The following computer abuses were put on the optional list: the alteration of computer data or programs, where such alteration does not constitute damaging; computer espionage implicating the violation of trade and commercial secrets; and the unauthorised use of computers or of a protected computer program. In quite a number of states, there has been an expansion of the criminal law to cover those cases referred to in the first offence. Opinions vary throughout the world on the question of whether and to what extent actions should be taken against violations of trade and commercial secrets using the means available under the criminal law. The question of criminal liability for unauthorised use of computers is largely connected with the question of whether and to what extent property in general should be protected against unauthorised use.

In the last-mentioned offence, the question of criminal liability is connected with an expansion of copyright law.

When putting these offences on the optional list, the committee agreed that these were areas to which the relevant legislative bodies should at any rate also give consideration when legislation is being planned in respect of computer-related crime. The committee refrained from including further examples of offences whose criminalisation has not found any echo in Europe until now (for example spying out a password that has not been stored or the trading in stored passwords). Reference can be made here to legislation in the United States.

4. The structure of the guidelines is based on a uniform pattern. First of all, the specific manifestation of a computer offence is portrayed and there is a general review of the applicable national law and its scope. This is followed by a description of the constituent elements of the offence and by an indication of the legal interest protected by the provision. A commentary then gives a detailed explanation of the offence and its essential elements.

The committee has deliberately chosen to use the words "without right". This notion is considered to be larger than the notion of "unauthorised" which does not, as used by the committee, include all aspects of undesirable behaviour, for example the violation of contractual relationships. This broad approach has been adopted by the committee, since it felt that it was up to the national legislator to take a more restrictive stance (see, for example, the commentary on the proposal concerning computer fraud on page 38). The fact that the word "unauthorised" is used in the heading of some offences (see Appendix I) does not have any significance. It is merely used there to give a convenient short form.

There is no express attention given to the form that culpability takes other than cases where a specific intentional element forms part of the offence (for example in respect of computer sabotage, where the intent to hinder the functioning of a computer or a telecommunications system is a constituent element of the offence). Non-reference to this subjective element means that there is criminal liability for intentional action only — as is also the case in some national criminal law systems. According to the continental conception, this will include *dolus eventualis*. Negligent and reckless conduct are not included in the guidelines since the committee felt that such conduct should not, as a rule, in respect of the offences described in the guidelines, be criminalised (see Chapter I.2).

5. Throughout this report, and especially in the guidelines for national legislatures, the committee uses certain technical terms such as "data",

"computer" or "computer system". According to the terms of reference, the committee should study and agree upon terminology. It was originally the intention of the committee to publish, as an appendix to the report, a glossary of terms which could be used especially for the purposes of interpreting the guidelines, and very valuable work in this respect has also been undertaken by one of the scientific experts, Professor de Schutter. However, the committee has finally chosen not to adopt any formal definitions. There are several reasons for this approach. Existing definitions, especially ISO standards, are elaborated for technical purposes but not for the purposes of interpreting penal law. The committee considers that the guidelines as well as new computer-crime legislation should be technology-neutral (see I.2). In addition, national definitions and standards are elaborated in several countries (the DIN norms, for example, in the Federal Republic of Germany) or by international organisations (for example WIPO). Such definitions and standards might differ to some extent. Furthermore, several member states have deliberately chosen not to define certain terms even when adopting new computer-crime provisions. It is often a question of legislative technique if a member state chooses to adopt definitions and it should therefore be left to individual states. Whenever the committee has found it necessary to give more ample information concerning a term, such as in the case of "topography" and "semi-conductor", explanations will be found in the commentary of the proposed guideline.

2. *Minimum list*

a. *Computer-related fraud*

Phenomenology and legal situation

Experience has shown that the assets represented or administered in computer systems (electronic funds, deposit money; see the development of electronic home banking, computerised stock-keeping and balancing of accounts, but also of cash dispensers, automatic teller-machines, electronic high-efficiency vending machines) have become the target of manipulations like traditional forms of property. Preventive safety measures have not been able to hinder property-damaging computer manipulations effectively enough. Although the registered number of such cases in member states and in other industrialised states is, except in the area of the misuse of automatic cash dispensers, not very high (Japan:

929 cases in 1985; Federal Republic of Germany: 440 cases in 1984), attacks against another's property by means of a computer usually cause remarkably high damage. The manipulations detected were (outside the cash dispenser area) mostly committed by insiders, by company employees or the working staff in public administration, often facilitated by the lack of sufficient control. The new crimes consist in new *modi operandi* of property violations, mainly brought about by input manipulations, that is, the feeding of a computer with incorrect data and, to a lesser extent, by program manipulations and other interferences with the course of data processing.

Practice shows that such offences are difficult to detect and sometimes cannot be prosecuted because of loopholes in traditional criminal law. Sections on fraud or equivalent offences often require the deception of a human being (with exceptions, for example, in Canada, France, the Netherlands and Scotland; the question is controversial in England and Wales, see the English report, p. 22). Other offences like theft, embezzlement, cheque or credit card fraud, breach of trust or unfaithful management usually have a limited scope of application (see the OECD report p. 30 *et seq.*). In many countries, provisions on theft and embezzlement require the existence of a corporeal object. Even if an offender withdraws money from a cash dispenser by a false input manipulation, it has sometimes been questioned — due to the technically limited possibilities to prove the legitimacy of the card-holder — whether the money was "taken" or "embezzled" against the will of the owner (for example by some courts in the Federal Republic of Germany). Credit and cheque card offences are not applicable to all types of modern money access cards. Therefore several member countries have felt it necessary to amend their criminal law by the extension of provisions on fraud or by the creation of a new offence on computer fraud (Austria, Denmark, Federal Republic of Germany, Greece, Norway, Sweden; see also similar proposals in Finland, Portugal and Switzerland). This reflects the common opinion that certain computer manipulations deserve punishment. The committee suggests that the following acts should be punishable:

Text

"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 with the in-

tent of procuring an unlawful economic gain for himself or for another person (alternative draft: with the intent to unlawfully deprive that person of his property)."

Protected legal interest

Property's integrity is to be deemed the main legal interest to be protected by this provision. But also trust in the security and reliability of transfer of funds by the means of data processing can — subsidiarily — be seen as an interest to be covered by the above provision.

Commentary on the proposal and its constituent elements

The general aim of this proposal is to criminalise any undue manipulation in the course of data processing in order to influence the latter's result for effecting an illegal transfer of property-damaging values. The proposal leaves it open whether this aim is reached by the interpretation of rather broad provisions of existing national law or by introducing amendments or even additional provisions.

Computer data and computer programs are the object of computer fraud manipulations. The restriction of the offence to "computer" data and programs reflects the supplementary role of a provision on "computer fraud", where data put, or to be put in a computer are misused.

The *modi operandi* are enumerated exclusively. To make sure that all possible relevant manipulations are covered, the constituent elements "input", "alteration", "erasure" and "suppression" are supplemented by the general act of interference with the course of data processing. The input covers data entries in computers. It may influence existing data processing or cause it to start. The text allows the conclusion that the offence includes the input of incorrect data as well as the unauthorised input of correct data. This would for instance mean that the provision does not only cover the misuse of stolen cheque and credit cards in a bank automat but also the misuse of one's own card by (manipulated) violation of the credit limits (covered in many countries by provisions on theft). It is up to the national legislator to choose a narrow interpretation concerning the latter case. He might prefer to consider it only as a breach of a civil obligation and put the risk on the card-issuing institution (see the French *Cour de Cassation*, 24 November 1983; the United States Credit Card Fraud Act of 1984 which does not include this situation; a trend towards decriminalisation is favoured in the *Report on decriminalisation*, European Committee on Crime Problems, 1980, p. 197 *et seq.*). Alteration, erasure and suppression of data or programs are included because they can lead to the same effect as the input of incorrect data. Alteration includes modifications, variations and partial changes. Erasure includes the removal of data from a data medium, for example, stored on magnetic tapes or other storage devices. Suppression includes the holding back and the concealment of data which may have the result that such data are not fed into the data processing as required for its correct application. An express restriction of the alternative "alteration" to cases of "deterioration" (see the provision on damage to computer data, *infra*) is not necessary, due to the fact that the subjective requirements produce the same result in the end. Interference with the course of data processing deals with other acts like hardware manipulations, acts preventing print-outs, acts affecting recordings, data-flow or the programs run in their temporal sequences.

The computer fraud manipulations described shall at least be criminalised if they influence the result of data processing in a way which produces a direct economic or possessory loss of another person's property and the offender acted with the intent of procuring an unlawful economic gain for himself or for another person, for example by an illegal transfer of funds or another thing of value.

The offence has to be committed intentionally which is commonly understood to include both *dolus directus* and *dolus eventualis*. The "intent" requirement can be understood in a narrower sense as this is done in some continental legislation, which requires a specific intent to procure an unlawful gain for the perpetrator or for a third person.

Other comments

It is of course incumbent upon the national legislator to choose a broader scope of punishability by redrafting the intent requirement at the end of the text of the offence in the light of the tradition in the sphere of property offences (see, for example, the solution of Anglo-American law).

b. *Computer forgery*

Phenomenology and legal situation

The manipulatory acts described in respect of computer fraud do not necessitate the objective of damage to property and acquisition of a pecuniary advantage. They may be associated in an extended sense with

unauthorised data storage designated to have a misleading effect on legal relations or with corresponding alterations made to stored data. Where stored report marks or personal status data are altered in a computerised register without authorisation, such data may thereby acquire a different evidentiary value and the course of legal transactions, which relies on the authenticity or correctness of the information contained in such data, may be subjected to a deception. Particular examples of computer manipulation of the non-property kind have come to light in various countries. Unauthorised inputs or alterations of computer data with evidentiary value, perpetrated in preparation for computer swindles, occur more frequently. Examples are illegal entries into the magnetic part of cash-dispenser cards.

In some countries, such acts can be subsumed under existing provisions on forgery of documents (the Netherlands, Norway, Swiss Supreme Court, 18 December 1985), because data recorded on electronic data-processing media, due to the fact that they could be read with the aid of technical devices, were considered to be equivalent to documents in the classic-traditional sense. In most countries, however, the provisions on forgery require visual readability of statements or declarations embodied in a document and therefore do not cover electronically stored data, which leads to gaps in criminal law (see the OECD report, p. 32). This is especially the case if the provision on forgery protects only signed documents and if electronic signatures are not of sufficient equivalence. Even as far as visible computer print-outs are concerned, there are additional problems as to whether they can be considered as forged documents if their content is essentially determined by the manipulated data-processing computer. Furthermore, the question may arise as to whether the print-out is a false document or just a genuine one containing incorrect statements of facts, a distinction which may play a role in several countries. Manipulations of stored data with evidentiary value have the same serious consequences as traditional acts of forgery if, for example, a third party is thereby misled. It would be unjustifiable for such data to remain exempted from criminal law protection in relation to forgery, although there would in fact be this protection against forgery if — as previously — they were recorded in a manner that is externally perceptible.

The aim of granting the same protection to such data as written documents has led, in England, to an extension — *vis-à-vis* forgery offences — of the notion of (false) "instrument" to include any "disc, tape or other device on or in which information is recorded or stored by electronic or other means", to amendments of the offence of falsification of documents

in Victoria (Australia) and, in the Federal Republic of Germany, to the creation of a new offence of falsification of data with evidentiary value and to amendments to different offences of forgery (see the OECD report, pp. 35-36).

The committee suggests therefore that the following acts should be punishable:

Text

"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."

Protected legal interests

The protected legal interests are identical with those protected by the traditional law of forgery: security and reliability of documents or other instruments which may have consequences for legal relations. Only the protected objects of action have been expanded. The reference to the traditional objects of forgery, made in the description of punishable conduct, avoids any closer contention with the range of protection afforded to documents, which varies greatly in individual member states. Hence the question may be left open as to whether a forgery of a document and a falsification of evidentiary data only take place where there is a deception as to authenticity, that is, as to the maker — in other words whether it is a matter of the document's telling a lie about itself as a document or whether falsifications of the content of the statements made therein, their correctness and veracity are also covered. The text merely requires the new possibilities of manipulation to be criminalised under national law in the same way as traditional forgery of documents.

Commentary on the proposal and its constituent elements

The proposal's aim is to put the falsification of data having probative force on the same footing as the forgery of documents or other instruments in criminal law terms. Extension of protection is only necessary in those states that demand direct perceptibility of the content of the data and of the maker in regard to forgery of documents.

The text proposal, as a minimum standard, refers to the same manipulations of computer data and computer programs as in the case of computer fraud. To this extent, reference is made to the explanations made there. As a result of these acts, there has to be a data situation which is similar to the forgery of a document or other instrument. Similarity will suffice because it follows from the nature of stored computer data that such data are not immediately perceptible in the same way as statements in a written document are. This also applies to the maker. So far as there are doubts under national law as to whether the traditional provision on forgery also covers falsification of probative documents produced by a computer, the latter should also be included through the proposed extension of criminal law protection. This also applies to those cases where the manipulated data are no longer printed out after processing but are used directly for further computer processing, as is particularly evident in the case of bank, accounting and payment transactions (for example through further use of data carriers at a different bank from the one making the input). It includes inducing a machine to respond to the false instrument as if it were a genuine instrument, which is parallel to inducing somebody to accept a false instrument as genuine (see Section 10.3 of the English Forgery and Counterfeiting Act 1981 which, however, was not applicable to a case of computer hacking in England, "the Prestel case"). Falsifications which mean, for example, the unauthorised input of data bringing about a data situation corresponding to the making of a false document and also subsequent alterations of data corresponding to the falsification of a genuine document are primarily covered here. In so far as the unauthorised use of a document forged by another person is also a criminal offence under national law, the unauthorised use of false data with evidentiary value should also be made punishable. The subjective conditions (intent) correspond to those of the forgery of documents.

Other comments

Difficulties in establishing who it is in data processing that corresponds to the maker of a document (is it the owner or the operator of the data-processing equipment or the person responsible for the program or the person entitled to make data dispositions or the person entering the data?) have sometimes led to reflections on the possibility of expanding criminal law protection beyond that afforded to documents. Considerations supporting such a step might be founded on the easier potentialities, in certain circumstances, for manipulating computer data as well as on the added difficulty in detecting such manipulations. Each national

legislature will have to decide for itself whether these reasons are enough for going beyond the parallel criminal law protection proposed.

c. *Damage to computer data or programs*

Phenomenology and legal situation

The economic value of computer data and programs, the dependence of companies and administrative authorities on data processing, along with the high concentration of data stored in electronic devices, make computer sabotage, unauthorised erasure, corruption or damaging of data a particular danger for business and administration. The proper functioning of companies and organisations as well as of social processes is particularly at stake here. Attacks on computer data and programs which are an end in themselves and not merely an element in a fraudulent scheme (for example for computer fraud or forgery) have become evident in member countries and in other countries as well. Although the number of known cases is not very high, damage or disturbances caused by this have sometimes been considerable. Data destruction may be the result of physical attacks on computer facilities by bombs, by specific sophisticated or even quite simple sabotage acts such as the erasure of data by magnets or by more computer-specific methods like tampering with a program, for example by the insertion of crash programs or so-called logic and time bombs. A most dangerous modification are virus programs which copy and implement themselves in other programs and data files, which can carry destruction routines.

In most of these cases, the purpose of the perpetrator is only to do harm. The intention of drawing a corresponding illegal profit from such an act is not necessary and it is not typical in this form of criminal conduct. It is possible, however, that an indirectly lucrative motive exists, for example the wish to do harm to a competitor. A common motive of computer damage is the revenge by an employee whose contract has been or is going to be terminated. Political or ideological motives are also typical, as in cases of terrorist acts. Finally, the motive of attracting public attention is also not infrequent.

For the above reasons, the creation of additional provisions referring to the act and its immediate effect on the software or the stored data rather than to remote consequences for the whole system is preferable in order effectively to protect such software and the data concerned from mischievous damage and interference. The necessity of amending the criminal law in those states where the acts are not already covered by the

existing law, or where the legal situation is unclear, is reflected by new provisions or amendments to existing provisions in Austria, Canada, the Federal Republic of Germany, France, Greece, the United States and in commission proposals or government bills in Finland, the Netherlands and Switzerland. This has led to the suggestion that the following acts should be punishable:

Text

"The erasure, damaging, deterioration or suppression of computer data or computer programs without right."

Legal interests protected

The legal interests protected may be said to be the integrity and the proper functioning or use of (stored) computer data or computer programs. One can criticise here, as too narrow, a minority view in the Federal Republic of Germany that the legal interest protected is the property as manifested in the special form of data and programs, even though the spur to the creation of criminal law provisions in this field may essentially have been the danger of impingement upon economic interests. A restriction tending in a similar direction is to be found in provisions of this kind in various United States jurisdictions, which choose, as the object of protection, a loose concept of property including data and computer programs as well; to be covered by this concept of property, however, they must be "anything of value". Data do not only embody information having a value of property; they may for example serve the securing of evidence, or relate to the private sphere, or concern computer operations.

The specific character of damage done to data means that – other than is largely the case with damage to property – it is not a matter of injuring the substance of an object and thus impairing its utilisation but rather a matter of altering the quality of the information in stored data and programs, which may obviously reduce their potential use.

The natural or legal person concerned has not only an interest that programs or data stored in computers remain complete or integral in a quantitative sense, but also that they remain unchanged in their state or condition in the qualitative sense, that they do not deteriorate, that is change for the worse.

The text as formulated does not solve the question of in whose interest the protection is provided. Is it in the interests of the person doing the storing, who may be entitled to dispose of the data (as, for example, the owner or the lawful possessor of the data carrier or as the person requesting that a certain work be carried out), or does the protection also extend to the interests of the person to whom the data content relates, where this person enjoys a right to the integrity of the data? The latter interest can be the object of statutory data protection provisions. At any rate, the text permits a broad interpretation, at the same time not excluding the possibility of separate regulation of the data protection law aspect in domestic criminal law.

Comment on the proposal and its constituent elements

The aim of the proposal is to provide computer data and computer programs with protection similar to that enjoyed by corporeal objects against intentional infliction of damage. This can be done by new provisions, by amendments to the provision concerning damage to property through new subsections or by equating damage to data with damage inflicted on corporeal property. Data and programs are protected in different stages, regardless of whether they are stored, processed or transferred by means of computer-automated equipment. The acts described require a negative effect on the state of data or programs in their capability of functioning according to the task assigned to them by the person disposing of them. Thus, erasures etc. that do not have these effects, that, for example, even improve or ameliorate the software or the data as regards the subjective purposes or that represent only an unauthorised interference, are excluded. The problem of whether the interpretation of the meaning of the several acts is determined by more objective or more subjective criteria is left to the national legislator.

The erasure of data is the equivalent of the destruction of a corporeal thing. It destroys them and makes them completely unrecognisable. This may occur through the destruction of the data carrier, through overprinting on magnetic tapes, through the blacking out of data and the erasure of necessary connections. "Damaging" and "deterioration" as overlapping acts relate in particular to a negative alteration of the information content of data and programs. They also include those cases which, in Canadian law, are described as "rendering useless or meaningless". A "suppression of data" occurs where the perpetrator causes them to disappear without them being erased, by giving corresponding instructions. They are removed from the access of the authorised persons and they can, therefore, no longer be used.

The different acts described above are only punishable if they are committed without right. This element is very important because one element of the parallel offence of "damaging property" – namely that the thing damaged "belongs to another person" – does not appear in the description of the new provision. In Western Europe the term "belonging to another person" will mostly be seen in relation to the notion of property in corporeal goods, which is not applicable to data. The function of this element can be taken over by the term "without right", understood in a broad sense and including persons who are not entitled to act as they did either in their own right or by authority of those who had a right. If one partner erases data without the necessary co-operation or consent of the other partner he acts without right. The same applies where a person authorised by the owner, an employee for instance, acts beyond or contrary to the instructions he has received. Persons who did not have a right, but believed erroneously that they had one, commit the offence but they may be excused in accordance with provisions on mistake of fact or law under the legislation concerned. As in the other offences, the offender must have acted intentionally.

Other comments

There is a strong relationship and even partial overlapping with the offences of alteration of computer data or programs without right and the hindering of the functioning of a computer, which will be discussed *infra*.

d. *Computer sabotage*

Phenomenology and legal situation

Disturbances in computer and telecommunications systems may have even more negative consequences than mere negative alterations of computer data or programs. Because of the increasing dependence of modern society on these systems, they play such an important role that the protection of the functioning of the systems is of great interest not only to the owners/users of them, but in many cases also to the public. Hindering the functioning of important public computer systems, for example military, medical or traffic control computers, or private computers, for example bank or insurance company computers, may not only have great economic consequences, but may also lead to disastrous human consequences. Where, for example, accounting operations are

brought to a standstill in data-processing centres, this may lead in individual cases not only to economic ruin for the operators of the data-processing centre but also to the economic ruin of the businesses working in collaboration with the centre concerned. The dangers to the economy resulting from cases of computer sabotage are to some extent estimated as being greater than those resulting from other cases of economic sabotage.

Preventive measures should also, in such cases, play the most important role, but it is necessary for these measures to be supplemented by criminal law provisions. Several of the member states of the Council of Europe have already enacted or made criminal law proposals on this subject. In many cases, such acts can be combated by wide interpretations of the offences on damage to property or through the application of the offences that have already been introduced in several member states on damage done to data and programs (see, *supra*, Damage to computer data). The new Danish, German and French laws have further provisions on "disturbances in the operation of data-processing systems". In Finland, a review of the offences on "causing public danger" is under way which would also include serious acts of computer crime. The Dutch Commission contains several proposals to enable the authorities to combat threats to the continuity of the functioning of information technology processes which are associated with general interests, and to punish assaults on information technology equipment with very grave real or potential consequences. Special provisions of this kind enable more severe sentences to be imposed than the offences on damage done to things or data. More extensive acts may also be included. The committee, therefore, recommends that the following acts be made punishable, as in the OECD report at p. 70:

Text

"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 telecommunications system."

Protected legal interests

The legal interests to be protected can be described as the interest of the owner and/or the user of a computer system or telecommunications system being able to have it function properly. So far, there is

great similarity to the legal interests protected by provisions against the damaging of data or programs (*supra* p. 43).

Commentary on the proposal and its constituent elements

It is important to notice that the essential part of the crime, as described, is the intent to hinder the functioning of a computer and/or telecommunication system. This is different from what could be called damage to computer data (*supra* p. 43). The constituent elements of the computer sabotage offence fall into two parts: 1. the means and 2. the aim.

The means can be any kind of interference with a computer system. The text mentions as examples the input, alteration, erasure or suppression of computer data or programs. These examples of acts constitute to a great extent — as far as they are carried out without right — the above-mentioned offence of damage to computer data. As this type of offence is explained separately, only partial reference is made (*supra*, p. 43). Differences stem from the differences in the protected objects. The object of computer and telecommunications systems calls for the general inclusion of acts of interference of which some examples are given and, in this respect, it goes further than the provisions against data damaging. As the input of false data or the unauthorised input of data may obstruct the functioning of such systems — just like interferences due to data alterations — this act is included, too. The term "input" is explained in connection with the offence on computer fraud (*supra*, p. 38).

The committee leaves it open to member states to decide whether all kinds of interference with a computer system should also be considered as criminal modes of committing computer sabotage. As examples of such interference with a computer system, which do not fall within the examples stated in the text, there could be inclusion of any kind of physical damage to the computer, switching off the electric power to a computer system or obstruction or interruption — for example by unauthorised use — of the lawful use of the computer system (all acts carried out with the intent to hinder the functioning of a computer system).

Some member states might feel it necessary — for instance because of national legislative traditions in similar legal areas — to make limitations as to special kinds of mode of interference with a computer system. It has, for example, been mentioned that strikes (lawful or unlawful) among people working in the computer section of a firm or a public authority may affect the functioning of a computer system. Also, other kinds

of omissions might affect the functioning of a computer system, but should not — depending on national legal traditions — be criminalised.

The aim of the perpetrator of the offence of computer sabotage is to hinder the functioning of a computer or telecommunications system.

The text leaves it to member states to determine the extent to which functioning should be hindered — partially or totally, temporarily or permanently (making a repair necessary). One type of act may for example only affect some parts of the functioning while the rest of the functioning is not affected by the act; an alteration of one program in a traffic control computer system may, for example, only affect a small part of traffic control. The choice might be affected by the fact that some countries may prefer to criminalise the different kinds of attacks on a computer system separately — for example as mischief to corporeal things (like physical damage to the computer systems) or as damage in relation to data or property — and only criminalise computer sabotage under aggravating circumstances — for example, only if the attack has resulted in the hindering of data processing of essential importance to the public (see Norway and the Dutch proposal) or to an enterprise (see the German solution) or where it has caused major disturbances in the operation of the computer system (Denmark).

The text leaves it open as to what kinds of computer or telecommunications systems should be protected by the provision. In principle all kinds of computer systems are protected — all from the biggest system to the smallest minicalculator. Depending on which other provisions in their respective national criminal codes would protect attacks on minicomputers, some countries may wish to make limitations as to the size, importance or kind of use of the computer or telecommunications system which should be protected by the criminal law against the hindering of their functioning.

e. *Unauthorised access*

Phenomenology and legal situation

Due to the increasing use of data processing in business and administration, valuable economic, administrative, governmental and private data are largely stored in data-processing systems and on data carriers. Specific developments in the computer world, the enormous spread of

personal computers and the great progress in telecommunications together with the new videotex systems and other interactive media, which make it possible to conduct dialogues with and between computers in different parts of the world, have led to new problems. They have created the media-favoured phenomenon of the "hacker" trying to get access to an organisation's computers to which he has no connection whatever. This is done from long range, using a microcomputer, acoustic coupler or modem, generally via the public telecommunications network. Hackers explore the capabilities of computers and communications, causing them to perform to their limits. Successful penetrations into computer and communication systems have occurred throughout the world. Opportunities for gaining access to vast amounts of data stored in one tiny physical space have increased. Sophisticated military and scientific computers have been broken into, as well as computers belonging to governments, banks and credit card management establishments, large health-care institutions, universities, etc., thereby endangering the protection of economic, scientific or personal data or of data of national security importance and mostly stored in data banks. There have even been transnational instances of hacking, from the United States and Germany to Canada and from Germany to Japan, France and the United States.

Pure unauthorised access to computer systems is mainly committed by young hackers, who have a variety of motives. They may intend to improve data protection; they may want to overcome the challenge of a company's security system; they may enjoy infiltrating data banks, or they may want to boast among friends or to the press. When some cases become public, these acts of hacking can be useful for the detection of loopholes in computer systems. However, in general, the committee considers them as dangerous because system errors, failures, blockades or even crashes may be caused; data may be destroyed by negligence, or security deficiencies, found by acts committed as a challenge, may subsequently be used for financial fraud or for the modification of stored data — as specific cases have revealed. The activity of hacking may give access to confidential data which the hacker may use to his own advantage. It is a kind of intrusion into computer privacy against which the same criminal law protection as traditional infringements of privacy should be enjoyed. In addition, hackers often avoid payments, for example with the aid of so-called "blue boxes", for the use of a system, either by mechanically blocking the counter or by deviating the charge for the call to another person's account (see the Scottish report, p. 4). In such cases, even the provisions of computer fraud might be applicable (see, *supra*, p. 36).

At present, there are few countries with legislation that can be used to punish behaviour which consists purely in gaining unauthorised access

to a computer network (Denmark, France, Sweden, United States). In some countries (such as Canada, Federal Republic of Germany, German Democratic Republic, Norway), at least those cases are covered where computer data (especially personal data) are illegally procured or intercepted (see this specific offence, *infra*). The committee is convinced that the dangers arising from acts of hacking may increase in the future and therefore proposes that all member states should undertake to prevent and combat such dangers, not only by improving security measures but also by criminalising at least qualified acts of so-called "computer trespass". It can refer in this respect, for example, to the reform proposal by the Dutch Commission. The Scottish Law Commission proposed the creation of an offence in respect of the unauthorised access to computer data or programs in order to inspect or otherwise acquire knowledge of the programs or the data or to add to, erase or otherwise alter the program or the data, with the intention of procuring an advantage for the offender or another person, or of damaging another person's interests. The English Law Commission discusses four different variants of a possible hacking offence. In a recent report on *Computer-related Crime and Criminal Law: An International Business View*, a working party under the auspices of the International Chamber of Commerce (representing 7 500 companies and business associations in 110 countries) suggested the introduction of offences in respect of unauthorised access to an EDP system (the ICC report). The committee suggests that the following act should be punishable:

Text

"The access without right to a computer system or network by infringing security measures."

Protected legal interests

The protected legal interest is, in the first instance, the security of the computer system, the inviolability of the "computer domicile". A parallel can be drawn with breaking into homes or offices, which has led to denomination of the offence as the electronic form of house-breaking (the Scottish memorandum, p. 25). In addition, the criminal law provision is supplementary to the offence on computer sabotage. On the other hand, a criminal prohibition of the unauthorised access is able to give protection, at an early indirect stage, against the dangers of computer manipulation, damage to computer data and computer espionage. It creates an obstacle to harmful acts which might follow intrusion into computer systems (see the higher punishments, where such consequences arise, in the French Act of 1988).

Commentary on the proposal and its constituent elements

The offence aims at preventing penetrations into secured computer systems or networks. Consideration might even be given to criminal law prevention of the mere unauthorised access to all computer systems, in other words, not having regard to whether they are protected or whether security devices are overcome (see the arguments for and against such qualifications in the Scottish and the English reports). For instance, such a requirement has been dispensed with in Sweden, the German Democratic Republic and the United States as well as in data protection legislation in respect of the offence of retrieving data. In the controversy concerning this offence's eligibility for criminal punishment, the committee considers the chosen limitation to be sensible within the meaning of a minimum standard. It avoids the risk of favouring managerial negligence in the setting up of suitable protection systems.

The objects of the offence are the computer system or networks. A computer network is a complex consisting of two or more interconnected computers. Access comprises the entering of the whole or any part of such systems. The method of communication (for example from a distance, including satellite links, or at close range) does not matter. The access is effected without right not only if it was obtained by a person exceeding his own entitlement but also if the access was not authorised by the person controlling access (see the Scottish report). Security measures can be infringed by being overcome or bypassed (see also the examples in the Dutch report). The kind of protective measures that are considered to be security measures, especially the required degree for the application of the offence, is left to individual member states. It goes without saying that the highest possible degree cannot be required. Otherwise, the criminal law provision might become inapplicable. Examples of security measures are mechanical or logical safeguards like passwords, built-in safeguarding programs and systems, or the use of cryptographic devices. The ICC report suggests that access through the unauthorised use of a password or by otherwise breaking the identification control or similar protection be made a criminal offence. It may be noted that the trading of passwords has been made a criminal offence in the United States.

In order to prove the infringement of security measures, it will in practice not be necessary to reveal elements of a company's security system, but essentially to prove the existence of the system at the time of the commission of the offence.

Other comments

Another alternative for qualifying the offence is to restrict its scope of application by subjective criteria relating to the behaviour of the offender, as alternatively proposed in the OECD report, p. 70 (dishonest or harmful intentions, see also the French Act of 1988 — *frauduleusement* — and the final proposal of the Scottish Law Commission). But it is of course up to the national legislature not to use such restrictions (see the earlier proposals in the Scottish memorandum). The supplementary protection granted by the offence of interception of data should also not be forgotten. It may, finally, be noted that the OECD report (p. 63) proposed that it could be considered to grant a "premium" in cases in which the perpetrator gives immediate notice of the access and of the loopholes used to the victim or to state authorities. Up to now, no state has, however, enacted any special provisions to this effect.

f. *Unauthorised interception*

Phenomenology and legal situation

Traditional kinds of espionage have now been supplemented by the new activity of computer or data espionage. Alongside the unauthorised retrieval of data, the tapping and monitoring of remote data transmission systems and the interception of data during transmissions or from electronic emissions, for example from terminals, have become possible. The interception of data communications in transit represents the same serious violation of the privacy of communications as the interception of oral or telephone conversations between persons. It can be considered as a new and modern kind of wiretapping. A specific form is the interception of the radiation and electronic fields surrounding the computer (terminal), for example for display on the eavesdropper's screen. The offence concerns a situation where the offender takes the data as they are without being able to manipulate them at will.

Traditionally, the statutes of many Western countries only apply in principle to the interception of conversations and, at most, to a limited extent to the interceptions of communications to, from and between computer systems. In some countries, especially in the United States, traditional property law (like theft) is applied to the "taking" of information by including computer data in the property concept or equating it to corporeal objects (see the OECD report, p. 40 *et seq.*). The differences in the nature of tangible property, of corporeal things and information as an intellectual value call for another solution. Such differences are also reflected in the specifics of so-called "intellectual property rights". They

are especially visible in the situation where data are illegally copied or recorded although their "owner" still has them. They have only lost their exclusive character. From the viewpoint of most member states a solution independent from property offences seems preferable (see the provision in the Federal Republic of Germany on data espionage; the proposals of the Dutch Commission). The committee therefore proposes to introduce, in addition to the offence of unauthorised access, the offence of unauthorised interception.

Text

"The interception, made without right and by technical means, of communications to, from and within a computer system or network."

Protected legal interests

The protected legal interests are the rights of undisturbed "privacy" (see Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms) and exclusivity of data communication. Depending on the means of interception the security of computer and telecommunications systems may be at stake.

Commentary on the proposal and its constituent elements

The proposal tries to extend the protection of oral and telephone conversations against tapping and recording to data communications to, from and within computer systems and networks. The object of the offence is communications, especially data transfer via public or other telecommunications systems but also including the private domain. The communication can take place inside a single computer system, between two computer systems belonging to the same person, two computers communicating with one another or a computer and a person.

Interception by technical means relates to "listening" to the content of communications, to the procuring of the content of data either directly, through access and use of the computer system, or indirectly, through the use of electronic eavesdropping or tapping devices. The requirement of the use of technical means is a restrictive qualification in order to avoid over-criminalisation. The committee is, on the other hand, convinced that the insertion of the requirement of "security measures", as in the previous offence (unauthorised access) would have limited the offence too much and made it inapplicable to serious cases of espionage in the field of telecommunications.

Criminal liability of course requires that the offender acts without right. The act is justified if the intercepting person has the right to dispose of the communicated data, if he acts on the instructions or by authorisation of the participants or the recipient of the transmission, if the data are intended for him or the general public or if — on the basis of a specific legal provision — surveillance is authorised in the interest of national security or the detection of severe offences by investigating authorities. Like the offence of unauthorised access, the act of unauthorised interception is only punishable if it is committed intentionally.

Other comments

The national legislature is free to increase the scope of application of a relevant criminal law provision. It may decide also to include the interception of a function of a computer system, for example by eavesdropping on inadvertent electromagnetic broadcasting of radiation from various components of such a system. Another example is the proposal of the Dutch Commission to punish the disclosure of the contents of transmitted data which were obtained by unlawfully tapping or recording.

g. *Unauthorised reproduction of a protected computer program*

Phenomenology and legal situation

Computer programs are one of the prime targets of computer espionage. The intensive investment of labour, skill, experience and time, the relatively high costs involved in the development of good computer programs worthy of intellectual property right protection on the one hand, and the easiness of copying such programs at low costs, on the other, are incentives for criminal activities. During recent years, the increase in computer crime caused by software thefts has been considerable in all industrialised countries. It accounts for the largest number of all computer crimes. It is, therefore, reasonable to provide not only civil law but also efficient criminal law protection against the unauthorised copying of computer programs and the distribution of such copies. Software assets are protected by a wide array of legal measures with differing scope of application. Patent law (including penal reactions) is only applicable, to a limited extent, to the technical side of computer programs (see, for example, Article 52 of the European Patent Convention and the Guidelines for Examination at the European Patent Office). Trade secret law (*infra*, p. 62) does not apply to the field of non-secret programs and, generally, cannot be used against third parties who acquire the secret in good faith.

Most industrialised countries now give computer programs the additional possibility of copyright protection, either by an extensive interpretation of existing law, by express amendments (see the OECD report, p. 48 *et seq.*) or by specific acts. The extent to which copyright law does apply to computer programs is a matter for each individual state. It is part of the responsibility of international bodies like the World Intellectual Property Organisation (WIPO) to aim at international harmonisation in this field. The consequence of civil law protection for computer programs is the application of the specific national penal provisions to this new form of intellectual property right. The commonly accepted hard core of criminally prohibited acts is reflected in Recommendation No. R (88) 2 of the Committee of Ministers on measures to combat piracy in the field of copyright and neighbouring rights. It has led to the following description of the prohibited offence:

Text

"The reproduction, distribution or communication to the public without right of a computer program which is protected by law."

Protected legal interests

The legal protection provided to computer programs as intellectual property shall guarantee that the investments in their development are worthwhile for the author of the program or the holder of the rights. It thereby serves as an incentive to such investments and fosters productive efforts which may have a positive and profitable effect on society, too.

Commentary on the proposal and the constituent elements

To a large extent, the proposal has already been realised in the national laws of the member states, thereby reflecting the necessity not only of civil law but also of criminal law protection. Computer programs are the object of protection. A broad definition was developed by the competent international body, WIPO, in 1978: Computer program "means a set of instructions capable, when incorporated in a machine-readable medium, of causing a machine having information-processing capabilities to indicate, perform or achieve a particular function, task or result". It is protected if it fulfils the requirement of originality. As copyright protection is related to the expression of ideas, the protectable subject matter is not the mathematical or technical idea, the algorithm, but rather its embodiment in a recorded program. Generally, source and object codes are capable of copyright protection. In some countries, a tendency to extend the limits can be observed (for example to include structure and sequence of a program, in the United States). Developments in this respect are among the tasks for national courts, national legislatures and international organisations. This applies, too, to the problem, for example, of determining the possible copyright protection of different phases of the development and of computer-generated programs.

The acts, which should at least be criminalised, are also prohibited by civil copyright law. Criminal law is to this extent necessarily accessory. "Reproduction" requires a fixation, for example, on a data carrier. Even the loading of a program from an external carrier into the internal memory of a computer may be considered as copying in terms of copyright law; if not, an amendment to copyright law might be given consideration (*infra*, p. 68). "Distribution" includes acts of sale or rents and other acts of copy circulation making it publicly available. National law may include additional acts like offers of sale etc., import, appropriation, use (see *infra*, p. 68) or even possession. These acts are punishable if they are done without right, that is, are not allowed by substantive law, and the offender acts intentionally.

h. *Unauthorised reproduction of a topography*

Phenomenology and legal situation

Semiconductor technology can be considered as being of fundamental importance for industrial development. The functions of semiconductor products depend in large measure on the invention, development and marketing of semiconductor integrated circuits called micro- or computer chips, the basis of which are their topographies, mask works or (original) layout designs. The development of such topographies and chips requires the investment of considerable human, technical and financial resources. On the other hand, they can be copied at a fraction of the cost needed to develop them. Without sufficient legal protection, aiming to suppress the manufacturing and marketing of unauthorised copies, lesser substantial investment in chip development might be the consequence.

There is a growing international consensus towards protecting a chip topography outside the framework of traditional law by *sui generis* legislation. In most countries, protection by copyright, patent, trademark, trade secret and unfair competition law is considered incomplete or at least as being unclear in its scope of application. The first specific law was the United States Semiconductor Chip Protection Act of 1984, quickly followed by the Japanese Act Concerning the Circuit Layout of a

Semiconductor Integrated Circuit of 1985. The third initiative occurred on the level of the European Community with the Council Directive on the legal protection of topographies of semiconductor chips, of 16 December 1986. This directive has been transformed into national law in several EEC countries, and in others the transformation is being prepared. In addition, reference is made to the new Austrian and Swedish Acts, to the Norwegian draft, the Finnish Bill and similar deliberations in Switzerland. Finally, mention should be made of the WIPO Treaty in respect of Integrated Circuits and its discussion in Geneva since 1985. The legal protection provided is supported in some countries by penal provisions, too (Denmark, Federal Republic of Germany, Japan, Netherlands, Sweden). In the light of the amount of investment involved, which is endangered by illegal copying and distribution without authorisation, and against the background of penal protection in copyright and utility model law, the committee recommends the introduction, in this area as well, of the following offence under national law:

Text

"The reproduction without right of a topography, protected by law, of a semiconductor product, or the commercial exploitation or the importation for that purpose, done without right, of a topography or of a semiconductor product manufactured by using the topography."

Protected legal interests

The legal interests to be protected are similar to those of the offence concerning the unauthorised reproduction of protected computer programs (*supra*, p. 55). The efforts of the original creator realised in this new form of intellectual property should be protected, it being also in the public interest to encourage further innovation.

Commentary on the proposal and the constituent elements

The formulation of the offence follows the description of the acts, in Article 5.1 of the Council directive, which the creator of the topography may authorise or prohibit (see also Article 4 of the WIPO Draft Treaty). The objects of protection are topographies of semiconductor products. According to Article 1.1.*b* of the Council directive, a topography shall mean a "series of related images, however fixed or encoded, representing the three-dimensional pattern of the layers of which a semiconductor product is composed, and in which series each image has the pattern or part

of the pattern of a surface of the semiconductor product at any stage of its manufacture". They are protected if they are the result of its creator's own intellectual efforts and are not commonplace in the semiconductor industry (Article 2.2 of the Council directive). A "semiconductor product" is "the final or an intermediate form of any product consisting of a body of material which includes a layer of semiconducting material, and having one or more other layers composed of conducting, insulating or semiconducting material, the layers being arranged in accordance with a predetermined three-dimensional pattern, and intended to perform, exclusively or together with other functions, an electronic function".

The topography itself is protected against unauthorised copying, sale, rental, leasing or any other method of commercial distribution, or an offer for these purposes (definition of "commercial exploitation" in Article 1.*c* of the Council directive). In addition, protection is granted against the unauthorised commercial exploitation or importation for that purpose of a semiconductor product (for example a microchip) manufactured by using the topography.

These acts are only punishable if they are done without right. This is not the case if the accused person can claim the application of legal provisions allowing him to copy etc., or if the creator of the topography has consented. The Council directive as well as national acts contain several important exceptions. They reveal that protection is not absolute. Examples are private reproduction for non-commercial aims, for teaching and research and so-called "reverse engineering", which allows copying for the purpose of discovering information allowing the creation of a competing topography. The exclusive right of commercial exploitation, not of copying, ends after the topography or the semiconductor product has been put on the market with the consent of the creator.

These exceptions show the limitation of the offence to clear cases of piracy. The offence should only be punishable if the offender acted intentionally.

3. *Optional list*

a. *Alteration of computer data or computer programs*

Phenomenology and legal situation

The erasure, damage, deterioration and suppression of data are discussed *supra*, p. 43. What cases are subsumable under the acts of "altering" (or modifying) computer data or programs, and are not already covered by the kinds of act named above (erasure etc.), is not immediately apparent. In an empirical study of data protection crime in the Federal Republic of Germany, no cases were found of illegal alteration of personal data to set alongside cases of illegal erasure of personal data. Reference can be made to possible cases in which the entitled person's interests have not been damaged, as, for example, when data or programs stored are not intended to suffer deterioration in their capability of functioning according to the destination assigned to them by their owner (as in the case of students tampering with computers in order to try their skills or to attract publicity). Probably more theoretical are cases where data or programs may even be improved as regards the fulfilment of the purposes of the entitled person. The independent scope of the acts termed as "alteration" (or "modification") correlates in any case with the interpretation of those designated as "damaging", "deterioration", etc. If the latter are interpreted narrowly — in particular, objectively rather than subjectively — this extends the scope of the act known as "alteration of data or programs". This kind of restricted interpretation is possible, especially where it is oriented towards a restrictive interpretation of the offence of wilful damage to property, for example where some effect on the substance of the tangible object is required. Over and above the inclusion of borderline cases, the practical significance of including the act of "alteration" may lie, above all, in the fact that it can free us from the need to ascertain the objective interests pursued and the subjective purposes of the owner when we are at the stage of assessing the act. This may, in the final analysis, be the reason why up to now, in relevant laws, there has almost without exception been express inclusion — alongside destruction and damaging of data — of cases of alteration (various United States states; Section 430 (1.1) of the Canadian Criminal Code ("destroys or alters data; renders data meaningless, useless or ineffective"); paragraph 21 of the Swedish Data Protection Act ("alters, obliterates"); Article 144 (2) of the Swiss Bill on the criminal law relating to property ("alters or erases")). Consideration should therefore be given to an extension of the offence on data damaging to include the following act:

Text

"The alteration of computer data or computer programs without right."

Protected legal interests

The legal interest involved is the protection against unauthorised interference with the usability of computer data or programs, thereby violating the interest of the person concerned in their continuing integrity. Otherwise, reference is made to p. 43, *supra*.

Commentary on the proposal and its constituent elements

The proposal takes up an internationally recognisable trend of including unauthorised alteration of computer data and programs in the protection provided by criminal law. The provision prohibits unauthorised alteration. The concept of alteration in the sense of modification or change acquires its meaning in connection with the requirement that such an act has to be done unlawfully, without right, etc. and in its relationship to the interest protected by the provision. Therefore, the alteration must be such that it changes the informational quality of the data or programs, usually to the disadvantage of the person concerned. Such a disadvantage is, for instance, the unauthorised infringement of or interference with the right of disposal of the data or the infringement of privacy. Examples of alterations are the addition of new data or combination with other data. The other prerequisites that the offender must have acted without right and intentionally are commented upon *supra*, p. 43.

Each member state remains, of course, free to frame the regulation more narrowly in its domestic criminal law (see the reference to the constituent element "damages" (*schädigt* in the Austrian Act, or restrictions in certain United States jurisdictions to "malicious" acts (California, New Mexico) or through the addition of "with intent to injure" (Minnesota)).

b. *Computer espionage*

Phenomenology and legal situation

Due to the increasing use of data processing in business and administration, company secrets and valuable know-how are now also stored, to a large extent, in data-processing systems and on data carriers. The advantages this entails have not, however, been able to prevent the misuse of these new techniques. The traditional kinds of industrial espionage

and violation of trade secrets have now been supplemented by the new activity of computer espionage. Its object can be either hardware, software or computer data. Besides theft and imitation of electronic data-processing equipment or of its components, "software theft" (see p. 55, *supra*) and data espionage are particularly viewed with concern in the business world. The spying out of enterprise data, on both the industrial and technical side (development and research data; production formulae; manufacturing processes; test results), as well as on the commercial side (company results; balance sheets; profit and costs calculation; turnover of merchandise; customer lists; suppliers' data; data on the organisation of sales; internal marketing studies; industry forecasts), can be equally advantageous for perpetrators.

The need for increased protection is undisputed today. One way to counter computer espionage as far as it relates to trade secrets is improved legal protection for trade secrets. The situation is similar to the application and improvement of copyright law to the copying and distribution of computer programs. The trend towards better civil and criminal law protection of trade secrets in the last twenty years (see the OECD report, p. 44 *et seq.*) has been a result of the increasing importance of economically valuable "information" in the development of science, technology and industry, being especially reflected in the increasing use of data storage and processing. Patent, copyright, design patent and trademark law are increasingly considered to be no longer adequate for giving sufficient protection in every respect to valuable know-how and confidential technical and commercial expertise. Traditional criminal law only suffices in certain areas (in those covered by the criminal law relating to property and the criminal law serving to protect national security or official secrets). Special provisions against so-called "embargo violations", granting protection against any exploitation or damage in military or economic terms to advanced technological developments, similarly, have only a limited effect when seen in relation to the whole field of trade secrets. The same is true of data protection laws. All this, including the conviction that civil law is not effective enough in various situations, has led to deliberations on additional and better criminal law protection. Since this area is not so closely related to the classical field of computer crime, and since, in the member states, there have been widely differing criminal policy assessments of the extent of the required criminal law protection of trade secrets, the committee has included it in the optional list. The following description of a criminal violation of trade secrets should be considered by national legislatures when reviewing relevant provisions:

Text

"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."

Protected legal interests

The violation of trade secrets is largely regarded as a violation of private economic interests which relate to the confidentiality of such secrets. The latter point has often led to a comparison with violations of the general right of privacy or even to their classification as such. Some authors give more stress, quite rightly, to the protection of the asset value of trade secrets as a product of capital and labour and to the protection of market competitiveness against the threat of illegitimate or unfair forms of espionage, betrayal and use leading to unfair competition. With the introduction of the computer, the ease of misappropriation, combined with the potentially enormous value of a compact body of information, has added immensely to the incentives for industrial espionage (*Report No. 46 on Trade Secrets*, by the Institute of Law Research and Reform, Edmonton, Alberta, and a federal provincial working party (Canada), 1986, p. 128). Development of the legal protection of trade secrets is, therefore, likely also to affect so-called "computer espionage" of stored trade secrets.

In shaping the framework for legal protection of trade secrets, a weighing up of the different interests involved has to be carried out. Too extensive protection might impair the mobility and the professional advancement of employees. The undisputed general usefulness of a free flow of information in Western societies (see the OECD Declaration on Transborder Data Flow, April 11 1985) puts limits on the protection of trade secrets in order to avoid a development which leads to an undesirable monopolisation of (stored) information and knowledge *per se* and to impediments for the spread of (technical) knowledge. Secret knowledge to be protected is, by its very nature, unstable. Its content is not absolutely protected as such, which has thus led to the notion of an "incomplete exclusivity right to the secret". If a third person acquires a secret without authorisation by the entitled person and publishes it, this can result in the loss of "secrecy" and thus also of the specific legal protection.

Commentary on the proposal and its constituent elements

The protected objects are trade and commercial secrets. Such secrets are constellations of facts of informational value standing in some relationship to a specific individual or corporate enterprise. These facts are objectively secret, that is not obvious or generally known. Access is only possible by a restricted circle of persons. Secrecy rests upon the will of the person running the enterprise (such will being objective and derivable from the circumstances, for example by the application of protective measures) having a justified economic interest in its maintenance. The historically determined restriction of protection in several countries to the technical production area is outmoded today. In the commercial sphere, too, there are secrets (see *supra*) whose preservation is just as essential to an enterprise. Thus, the text expressly mentions two kinds of secrets which shall cover commercial and industrial secrets.

The (economic) value of trade secrets can be endangered by different acts of condemnable behaviour, by their disclosure, transfer or their use without right or by their acquisition by improper means. As a result, the proposal follows a tendency in more recent legislation to include more and more persons in the circle of possible offenders. Especially as far as disclosure and use are concerned, the proposal includes not only (former) employees of the enterprise concerned, but also persons in senior positions, persons working together with a firm, licensees and even persons who acquire knowledge of trade secrets in the course of carrying out checks and examinations or as a result of communications made. In addition, all those persons may be included as offenders in respect of disclosure or use who have acquired the secret in a dishonest manner, whereby the act of a third person may suffice.

Besides the act of "disclosure" the text mentions the act of "transfer". The latter refers more to the transmission of a secret to a third person, whereas the former also encompasses communications made to the public. The "use" of a secret refers to its advantageous commercial exploitation.

Apart from the subjective criteria (*infra*), the scope of the offence is to a large extent determined by the discussion of the circumstances under which "disclosure" and "use" are "without right or any other legal justification" or of when a trade secret is acquired "by improper means". The proposal does not take the global approach of the Model Act of the Consultative Assembly of the Council of Europe (see Resolution 571, 1974).

The first two alternatives are certainly applicable if the "disclosure" or "use" violates a statutory or contractual duty to keep the secret. The same applies where the trade secret is acquired with the knowledge that it has been misappropriated, or acquired knowingly by, or as a consequence of, an offence, a violation of the law or of moral standards (*contra bonos mores*), that is, forming the basis of the so-called offence of receiving or handling of secrets in several member states. In cases in which someone has acquired another's trade secret in good faith but learns about its unlawful origin afterwards, it is for the national legislator to extend the applicability of criminal law.

The possible conflict between the interest of the owner of an enterprise in seeing his secrets preserved and the interests of employees in avoiding a loss of mobility or promotion chances can be solved by interpretation, too. It is not necessary to exclude altogether the application of the offence of disclosure or use to former employees bound by (reasonable) contract clauses for the protection of secrets; such an exclusion would lead to privilege for such employees in comparison with other types of offenders. If the terms of the contract of employment and the provisions of labour law can be interpreted in such a way that the utilisation of specific expertise acquired has not entailed any violation of an employer interest which merits protection, then the criminal law, too, can go further. Usually, the personal skill and experience of an employee do not form part of the information protected as trade secrets. The law relating to contracts of employment is also well suited to putting a brake on unreasonable post-contractual obligations to protect classified material. What is authorised or justified by civil law is authorised or justified in the application of criminal law, too.

The offence of "acquisition by improper means" follows international tendencies towards strengthening criminal law protection against espionage. The text does not go so far as to criminalise all instances of economic espionage, but restricts it to obviously reprehensible cases. This includes not only cases of theft of articles representing trade secrets, but also acquisition by bribery, by devious tricks, by secret illicit copying, by overcoming security devices or by application of technical means, including the retrieval and acquisition of secret data stored in computers or on data carriers, or at the stage of transmission.

A restriction of criminal liability is achieved by requiring not only that the offence be committed intentionally, but also that the offender must have acted with intent to cause economic loss or to obtain an unlawful economic advantage. The requirement of intent reflects the approach taken in all member states.

c. *Unauthorised use of a computer*

Phenomenology and legal situation

Known cases on the mere unauthorised use of data-processing systems ("theft of services", "time theft") are rare, but the number of unreported cases is nevertheless estimated to be rather high. Company employees, administrative staff, university professors and students were the main offenders. The objects of their activity were mostly use of the computer services of processing, storage and transmission. Unauthorised use often has to be regarded as a trivial conduct which does not cause any damage at all or no considerable damage. Students who do not strictly observe their computer-time allocations are a common example. However, there may be cases where considerable economic harm is caused by the illegal use. This is, for example, the case where the company's account numbers or rented computers are used in circumstances where there has to be payment for actual time spent thereon or when the company loses its services or customers by a blockade system or by the "blocking" of its employees' work.

To some extent, unauthorised use of computers is covered by other provisions on the minimum rules list, for example, unauthorised access or — in cases where services are obtained by data manipulations — by the provision on computer fraud. Due to the fact that not all cases are covered where extensive damage may occur, there may be a need for special provisions. It should, however, be underlined that in connection with this offence punishment should be the last resort, and that implementation of security measures and the use of labour contractual or disciplinary law remedies are important. How far a member state will go in introducing penal measures in this field will, to a large extent, depend on the general notion concerning punishment of the unlawful use of things. In the Scandinavian countries in particular, there exists a broad approach which does not rule out the inclusion of specific offences with qualifying elements and higher penalties. The Dutch Commission discussed the introduction of a similar offence but also with the qualification mentioned below (both loss and harm required). There are, however, many member states which do not recognise a general offence of this kind but only some exceptions in specific areas. Due to the different assessments of criminal policy in this area, different formulations for an offence on unauthorised computer use are put forward for discussion:

Text

"The use of a computer system or network without right, that either:

i. is made with the acceptance of a significant risk of loss being caused to the person entitled to use the system or of harm to the system or its functioning; or

ii. 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

iii. causes loss to the person entitled to use the system or harm to the system or its functioning."

Protected legal interests

The legal interests to be protected are of two kinds: on the one hand, protection of the economic interests of the entitled person and, on the other hand, more generally, the protection of the security and proper functioning of the system.

Commentary on the proposal and its constituent elements

The proposal contains three alternatives, which differ as to the extent to which the intentional "use without right" should be made punishable. They reflect the approach of the majority of the member states that the mere unlawful use of a computer deserves no punishment, especially when there is no real danger of harm or damage (for example the temporary use of a programmable pocket calculator, the use of energy being negligible). The act of "use" itself can be interpreted in a broad sense; the offence is restricted by additional elements. The offender must have acted without right. This requirement will be met when the user has got no authorisation at all, or when he has gone beyond the authorisation received. Whether the use should be characterised as unauthorised or not will in most cases have to be decided under civil law. This applies especially to cases in which the perpetrator is an employee who has gone beyond what he is entitled to do during the performance of his duties. In these cases, the internal regulations of the enterprise will be decisive as far as the right

of the perpetrator is concerned. In the situation described in the alternatives, it is supposed that the offender acts without right.

The restrictions in the three alternatives are twofold. They relate to a (possible) — economic — loss to the person entitled to use the system and to (possible) harm to the system or its functioning (amounting to considerable impairments). The most dangerous forms of unauthorised computer use can be countered with this distinction. The proposal allows the choice between a narrow alternative, requiring actual loss or harm to occur, and broader alternatives. The latter require either that a risk of loss or harm was caused by the unauthorised use or that at least the offender acted with the intent to cause loss or harm. A combination of different alternatives is also possible.

d. *Unauthorised use of a protected computer program*

Phenomenology and legal situation

The use of a protected computer program not acquired with the consent of the author is conduct that may be considered just as reproachable as receiving stolen goods. If, for example, a car-manufacturing enterprise acquires, in ways that cannot be traced, a protected computer program that instructs its robots to build cars, the continuous use of the program does not necessarily amount to copying in all member states. In some member states, however (for example, according to the prevailing opinion in the Federal Republic of Germany), the loading of a program from an external carrier into the internal memory of a computer is considered to be copying in the sense of copyright law. The author of the program might lose a substantial profit, which he would be entitled to if the car-manufacturing enterprise had acquired the program by regular means. Thus, the national legislature might consider expressly extending civil and criminal law protection of protectable computer programs to acts of unauthorised use. This leads to the following proposal:

Text

"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."

Protected legal interests

In this respect, reference is made to p. 55, *supra*. The proposed amendments would give protection against a specific infringement of a particular intellectual property right and of the values inherent therein.

Commentary on the proposal and its constituent elements

The aim of the proposal is to supplement the penal protection of computer programs that are amenable to copyright, which presupposes a corresponding addition to the civil law rules. It violates the rights of the author of the program more than the reading of a book printed by infringing a copyright, or the listening to a tape with music which is copied illegally, or the use of a tool manufactured by infringing a patent right; behaviour which obviously should not be criminalised. The danger of economic losses caused by the unauthorised use of a computer program is much higher than in these situations. The objects of the offence are such computer programs that have been reproduced without right. All forms of use without right are included. Rights to use conferred by the author or exceptionally allowed by substantive copyright law (for example for private use, which is, however, prohibited in several states) exempt the user from punishment. Punishment should be restricted to cases where the offender acted with the intent to acquire economic gain or to cause harm.

III. Procedural law problems

1. *Introduction*

In all industrialised countries until now, the legal discussion on computer crime focused on substantive law and neglected procedural law aspects. More than a dozen countries have created new laws or amended old ones, thus fighting computer crime by using substantive criminal law (see I.2), whereas only a few countries have enacted new legal provisions concerning investigations in computerised environments. Similarly, in most countries, there are several court decisions, books and articles on the substantive law aspects of computer crime, but only a few decisions and studies deal with the relevant procedural law.

A more detailed analysis of the procedural law problems is necessary. Computer-specific procedural law aspects are important not only for the prosecution of computer crime cases, but also for the investigation

of traditional offences, which to an increasing extent require the collection and use of computerised data. At present, this is especially illustrated by investigations of traditional economic crime, mainly in the banking area, where most of the evidence is stored in computer systems. In the future, computer-generated evidence and the respective legal problems will be of even greater importance due to the growing use of computers in all areas of economic and social life. Consequently, the following items are relevant not only to the prosecution of computer crime but to all kinds of criminal investigations in computerised environments.

In order to initiate an international legal discussion of the procedural law aspects, the following chapter will discuss three main topics associated with collecting and using evidence in computer environments:

1. The coercive powers of law enforcement authorities to gather evidence;

2. The specific legal problems of gathering, storing and linking personal data in criminal proceedings; and

3. The admissibility of evidence consisting of computer records in criminal court proceedings.

These three topics raise new computer-specific problems which, in addition, are also relevant to the functioning of international mutual assistance. However, the chapter does not deal with the more general procedural law aspects which are not specific for the prosecution of computer crime or for investigations in computerised environments, such as mandatory duties of witnesses to report specific crimes or the calculation of prescription for specific acts (for example permanent program manipulations or "logic time bombs" for computer sabotage resulting in damage). The same holds true for the confiscation of tangible property (such as data carriers) and intangible property (such as financial interests) since, until now, there has been no need to consider a specific and further-reaching "confiscation of data or information". The present chapter also does not deal with the practical problems of investigation agencies in computerised environments (for these questions, see Sieber, *The International Handbook on Computer Crime*, 1986, pp. 139 *et seq.*).

2. *The coercive powers of law enforcement authorities to gather evidence in computerised environments*

Successful investigations in computerised environments require a variety of information. Usually, the main object of interest is computerised data stored on corporeal data carriers. In addition, computer-specific

knowledge, the skills and co-operation of computer specialists and computer users are necessary, if the police is not familiar with the computer hardware or software, the security system, or its codes and passwords. In specific cases, the gathering of data transferred by telecommunications lines as well as permanent registration of computer operations might be needed.

The difference between the various types of information is essential since the criminal procedural laws of all European countries are based on a differentiated enumerative system of specific coercive powers. With respect to the above-mentioned requirements, most continental European systems differentiate between:

- the powers of entry and search of premises;
- the powers of seizure;
- the duty of witnesses to testify;
- the duty of witnesses to produce existing evidence; and
- the powers of wiretapping.

Additional provisions or reform proposals providing the duty of witnesses to generate specific computer print-outs exist only in some countries.

In most countries, it is questionable whether or not the above-mentioned 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 telephone communications between humans and not especially designed for intangibles and the special needs of the computerised information society. However, in many countries, there are no court decisions or scientific studies concerning these questions.

An international comparative analysis of the relevant questions raises additional difficulties. Firstly, the various legal systems concerning investigations in criminal matters and their 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 in the various legal systems and, consequently, influences the adaptability of the various legal provisions to the new challenges of the "information society". Thirdly, in many European countries, it is unclear whether or not an analogous interpretation of the criminal procedural law is possible. Consequently, and in view of the committee's terms of

reference, the following chapter can only give a first overview in order to initiate a more extensive international discussion.

a. *Search and seizure of data stored or processed in data-processing systems*

In practice, search and seizure of data stored or processed in data-processing 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 discs, tapes, cards or paper listings. In other cases, the data may be permanently stored in fixed disc devices or in chips which cannot be easily taken away from the computer installation. In specific cases (such as data scrolling on a screen or stored in the core-storage for a short time only), the data may not even have a permanent embodiment in a corporeal data carrier.

In most countries, the traditional powers of search and entry of premises as well as the traditional powers of seizure (which are often coupled) do not pose specific problems. Collecting these data stored or processed in data-processing systems, in most cases, first requires entry to and search of the premises in which the computer system is installed ("powers of search and entry of premises"); secondly, it is then necessary that the data can be seized or captured ("powers of seizure"). With respect to the investigation of computer data permanently stored on a corporeal data carrier, it has been advocated that the fact that the powers of search and seizure in many countries are directed towards the search and seizure of (corporeal) "objects" relevant to the proceedings does not pose serious problems, since the right to seize and to inspect the corporeal data carrier should also include the right to inspect the data. In other words, there is no difference between data that are fixed with ink on paper listings and those fixed by magnetic impulses in electronic data carriers. This result is even more evident in countries in which the powers of search and seizure are directed towards "anything" that would be admissible in evidence at trial (for the latter see, *infra,* section 3). There should, in any case, not be a difference in treatment between the two ways of storing information. If a document may not be seized because of a special provision, because, for example, the holder of the document may not testify as a witness concerning the contents of the document (the holder is a doctor, lawyer, etc.), then the same treatment should be given to computerised data.

Consequently, the application of the traditional powers of search and seizure might, in general, only cause problems if data are not permanently

stored on a corporeal data carrier. The same holds true in cases in which the legal principle of minimum coercion or of proportionality makes unlawful the seizure of comprehensive data carriers or complete computer installations in order to gather only a small amount of data. Uncertainties may further arise in cases in which data carriers (such as the core-storage, fixed disc devices or chips) cannot be taken away and be evaluated on a police computer but must be analysed by using the computer system being searched. For the latter case, it is unclear in most legal systems to what degree the powers of search and seizure include the power to use technical equipment belonging to a witness or to the accused. Only some legal systems clearly state that, in the execution of the search and seizure, all "necessary measures" may be taken.

With respect to searches in computer networks, limits and safeguards should be developed in relation to specific networks and connected computer systems and the persons involved in the investigation. The search of an undefined number of computer systems connected via telecommunication lines should be avoided. If the judge has not expressly granted more extensive search powers, then the search should be at least limited to what would have been allowed for the user of the system himself.

In conclusion, the committee recommends, therefore, that the member states consider clarifying the legal situation by amending their procedural law in the cases mentioned above.

The remaining uncertainties are solved by a proposal of the Dutch Commission permitting that: "Any data which could serve to reveal the truth shall be liable to be gathered or recorded, in so far as they are stored, processed or transferred by means of a computerised device." Such a *sui generis* provision for "gathering data" has the advantage of solving specific questions of "search and seizure of data" in data-processing environments, such as the reimbursement of costs.

b. *Duties of active co-operation*

The aforementioned powers of entry, search and seizure and even a *sui generis* power of gathering data, in many cases, do not guarantee a successful investigation, since the authorities often do not have the skills necessary to access modern data-processing systems successfully. Inasmuch as knowledge about computer hardware, operating systems and standard software is required, these problems can be solved by a better training of investigation officers (see Recommendation No. R (80) 3 by the Committee of Ministers on teaching, research and training in the field of

"computers and law"). However, access to data-processing systems also faces specific problems originating from the complex nature of modern information technology, which can only partially be solved by a better police training. This is especially the case with respect to specific security software and encryption intended to prevent unauthorised access to information. Consequently, the duty of citizens to co-operate with the police becomes of much greater importance in computerised environments than in a non-technical, "visible" area.

The legal systems of most Western countries include two legal instruments which might be used to reach the necessary co-operation in order to gather evidence in a computerised environment: the duty to hand over seizable objects of evidence and the duty to testify. In some countries, additional and further-reaching provisions or reform proposals have been enacted or suggested.

The duty to hand over seizable objects is often coupled with the powers of search and seizure. In most countries, the holder of a seizable object is obliged to hand it over on request to the (judicial) authorities; only some legal systems do not provide such an obligation. The duty to hand over seizable objects can help the investigation authorities, especially in selecting specific data carriers among the many tapes and discs which are usually stored in a computer centre. However, in many countries, the obligation does not seem to include the duty to print or generate specific information stored on a data carrier, since the respective legal obligations are directed only to the production of existing corporeal objects. An analogous application of these provisions permitting the production of specific information seems doubtful, since the exclusive enumeration of coercive powers in criminal procedural law is an essential principle of the protection of civil liberties. The same holds true for an analogous application of the duty to generate computer data according to tax and company law.

However, in many cases, an important duty of active co-operation can be based on the duty of witnesses to testify. In some countries, this duty to testify ("to tell the truth", "to answer questions", etc.) can be used successfully in certain phases of the proceedings, for example, to find out a specific password necessary to access a computer system or to locate specific information in large data storages. To a certain extent, it might also be possible to use a series and/or combination of questions to get explanations on the functioning of a difficult security system. However, in most legal systems, the traditional duty to testify cannot be extended to include the duty to co-operate efficiently nor, especially, does it include printing out specific information. Furthermore, it should be considered

that, in other countries, the witness has to testify only to the court (and in some countries to the public prosecutor) but not to the police which is, in actual practice, conducting the investigation. Only in a few (especially Scandinavian) countries does the traditional duty to testify contain the further-reaching obligation of the witness "to refresh his knowledge of the case, for example 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 to the Court".

In order to make investigations in computerised environments more efficient, a few countries have enacted or suggested new compulsory duties to generate specific information. According to the new 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." Similarly, the Dutch report suggests a new provision which does not only permit the examining magistrate "to gather or record any data liable thereto" but also to "require such data to be produced in a form determined by him". A similar proposal is also being prepared in a new Canadian bill.

The question of whether or not such duties to generate and hand over computer print-outs should be recommended is difficult to judge. On the one hand, a too intensive intrusion of the state into the citizens' rights must be prevented. On the other hand, it has to be considered that the complex nature of computerised environments generally leads to specific information problems which can be extremely detrimental to criminal investigations. It should also be taken into account that duties to generate specific computerised data do exist in other areas of law, for example in tax law and company law. The committee is of the opinion that this merits further consideration, in the light also of possible rights of the suspect to refuse active co-operation and his rights against self-incrimination.

c. *Wiretapping of telecommunications systems and eavesdropping on computers*

The tapping of telecommunications lines or computer systems can support criminal investigations, especially in cases in which data are only transmitted and not permanently stored, in which data are just crossing a country or in which a permanent observation of telecommunications or computer activities is necessary. Whereas the powers of entry, search

and seizure usually constitute a single, "visible" interference with civil liberties, the tapping of telecommunications and computer systems (analogous to eavesdropping) is generally a permanent intrusion which, in most cases, is not noticed by the citizens concerned.

Consequently, in most countries, the statutory requirements for telephone tapping and the recording of telecommunications are much stricter than for other coercive measures.

However, even with respect to telephone tapping, the legal situation differs considerably in the Western countries. In several countries, the principle of the inviolability of telephone communications derives from constitutional guarantees of confidentiality of correspondence and respect for privacy, rights which are also embodied in the Convention for the Protection of Human Rights and Fundamental Freedoms. In other countries, the inviolability of telephone communications is established by acts governing the administration of the telephone service and/or by criminal provisions prescribing penalties for the interception of telephone communications. The exceptions to the principle of inviolability of telephone communications also vary: in many Western countries, there are precise legal requirements for telephone tapping. In other countries, telephone tapping is based on general clauses. Some proposals resort to an analogous application of powers to intercept communications in the form of letters and telephone conversations. Other countries even practise telephone tapping without any legal justification. Finally, there are legal systems which consider any telephone tapping as illegal (for details, see Council of Europe, *Legislative dossier No. 2, Telephone tapping and the recording of telecommunications in some of the Council of Europe member states*, Strasbourg, May 1982).

It is essential to take into account the relevant judgments of the European Court of Human Rights in the context of wiretapping. In the Klass case, and subsequently in the Malone case, the Court emphasises the need for adequate and effective guarantees against abuse of secret surveillance carried out by public authorities, since such measures constitute a breach of Article 8, paragraph 1, of the European Convention on Human Rights and must be justified in accordance with the strict requirements of Article 8, paragraph 2, of the European Convention. In particular, the legal basis for wiretapping must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence.

The question as to whether or not the traditional powers of wiretapping can be applied to tapping other telecommunications services and computer systems is answered differently in the various countries. No computer-specific problems arise in legal systems in which the statutory law permits, for example, the "surveillance of the telecommunications traffic, including the recording of its content".

Computer-specific problems of interpretation however exist, especially in countries which only permit the "monitoring of conversations" or the "surveillance and recording of the telecommunications traffic on sound carriers". Such provisions are particularly problematic if an analogous application of coercive powers in criminal procedural law is not accepted. In order to avoid interpretation problems, some countries have already enacted or proposed new legislation making it possible to tap all kinds of telecommunications under the same conditions as for tapping telephone conversations. Such clarifications are to be recommended, since telecommunications between computers do not merit more protection than telecommunications between persons.

However, the respective coercive powers should be worded precisely and be harmonised to a greater extent in the various European countries. The committee considers it important, especially in the light of the European Convention on Human Rights and the practice of the Court, that these questions are closely monitored and considered further with a view to harmonising the various coercive powers that exist.

3. *The legality of gathering, storing and linking personal data in the course of criminal proceedings*

The legal requirements for gathering, storing and linking personal data vary considerably in Western countries. The differences between the legal systems are not only differences of substantive law requirements. They also concern the constitutional background, the legal hierarchy and the legislative technique.

An extensive discussion of the underlying constitutional requirements for gathering, storing and linking personal data exists only in a few countries. For example, in the Federal Republic of Germany, the Federal Constitutional Court, in its famous "Census-Decision", recognised that the state's storage of personal data (especially in computer systems) could influence the citizens' behaviour, endanger their general liberty of action and must, therefore, be considered as an infringement on civil liberties, requiring an express and precise legal basis. This approach is also followed in the Netherlands. The new Spanish Constitution and the new

revised Portuguese Constitution even contain specific safeguards protecting the citizens' privacy against the risk of modern computer technology. On the other hand, in many other countries, such as Denmark or France, the gathering or storing of personal data is not (yet) considered to be of constitutional relevance but is only dealt with by the legislator in statutory law.

The European Court of Human Rights has also been recently called upon to rule on the compatibility of collection and storage of personal data, without the data subject's knowledge, with Article 8, paragraph 1, of the European Convention on Human Rights. In the Leander case, the Court ruled that such a practice raised an issue under Article 8, paragraph 1, which fell to be justified under Article 8, paragraph 2. Other decisions of both the Court and the Commission have recognised that data protection falls within the scope of the right to private life guaranteed by Article 8.

Countries regulating the legality of gathering, storing and linking of personal data do it on a constitutional or statutory basis and, in the latter case, they have the choice to place the provisions in various contexts and laws. A few countries locate — at least some of — the provisions in their criminal procedural law. This legislative technique has the advantage that the criminal procedural code remains the exclusive enumeration for any infringement of civil liberties in the course of criminal prosecution. However, most countries — uniquely or partly — regulate the legality of police files in their general data protection acts; in the majority of cases, the provisions are applicable both to the repressive activity of the police (prosecution of crimes) and to its preventive action (maintenance of public order). Some countries exclude police files — completely or partly — from their general data protection laws and/or create specific acts for all types of (repressive or preventive) police data. Italy has a specific law governing police files, and the Netherlands will shortly adopt one.

Independently from these questions of hierarchy and context of the statutes, the legislative technique, the content and the control mechanisms of the provisions also vary. With respect to the legislative technique, some countries consider a more detailed and precise regulation necessary; other countries resort to more or less general clauses. There are also countries without any legal provisions (enacted by parliament) regulating the use of personal data in the police sector, for instance Belgium. As far as the contents of the laws are concerned, serious limitations seem to be applicable to police files in only a few countries. On the

contrary, with respect to registers of criminal convictions, in many countries, there are far-reaching and precise regulations on the deletion of entries. According to Recommendation No. R (84) 10 by the Committee of Ministers on the criminal record and rehabilitation of convicted persons, governments should take appropriate measures to protect information contained in criminal records, particularly when it is computerised.

An international comparison of these issues has been undertaken and efforts made towards an international protection of individuals by the Council of Europe. However, Article 9 of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (European Treaty Series, No. 108) allows derogation from certain provisions in the interest of protecting, among others, state security, public safety or the suppression of criminal offences. In 1987, the Committee of Ministers adopted Recommendation No. R (87) 15 regulating the use of personal data in the police sector. It lays down a series of guidelines for the governments of member states on ways of approaching issues raised by the collection, storage and processing of personal data by the police, so as to avoid a legal vacuum being created by invocation of the derogation envisaged in Article 9 of the convention.

4. *Admissibility of computer-generated evidence in court proceedings*

The admissibility of computer-generated evidence is not only important for the use of computer records in criminal and civil trial process. It is also essential for the extent of the above-described coercive powers and for 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 print-outs 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 print-outs and computer data can easily be manipulated (a phenomenon which is illustratively described as the "second-hand nature" of computer print-outs).

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.

The law of several countries, such as Austria, Denmark, the Federal Republic of Germany, Finland, France, Greece, Italy, Japan, Norway, Portugal, Spain, Sweden, Switzerland and Turkey, is based on the principle of free introduction and free evaluation of evidence (*système de l'intime*

conviction). In these countries the courts, in principle, can use all kinds of evidence and must weigh the extent to which it can be relied on. Legal systems based on these principles, in general, do not hesitate to introduce computer records as evidence. Problems occur only when procedural provisions provide specific regulations for the proof of judicial acts or proof with legal documents. In these cases, the content of a document could be regarded as a "copy", with the consequence that the court may inquire into the underlying data, as it is generally more reliable.

Contrary to the legal situation in these countries, the common-law countries, especially Australia, Canada, the United Kingdom and the United States, 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. However, there are several exceptions to the hearsay evidence rule, such as the "business records exception", or the "photographic copies exception". 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.

In these countries, the question as to whether computer files and print-outs are inadmissible hearsay evidence or fall under one of these exceptions has been the subject of extensive debate. Some common-law countries have accepted computer print-outs as falling within the business records exception. Others have elaborated laws and bills allowing computer records to be admitted as evidence if certain conditions are met.

The United Kingdom Police and Criminal Evidence Act, 1984, 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 (...) are satisfied."

In the United States, several state laws contain provisions which specifically address problems of evidence. In 1983, the Evidence Code of California was amended by a new Section 1500.5, which is identical to Section 3 of the suggested state legislation of the State Governments Committee. The new section provides 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 that they purport to present. This presumption, however, can be overturned by another party. If any party to a judicial proceeding introduces evidence that such a printed representation is inaccurate or unreliable, the party introducing it as evidence will have the burden of proving, by a preponderance of evidence, that the printed representation is the best available evidence of the existence and content of the respective computer information or computer programs. In Iowa, the new computer crime law of 1984, in Section 716.A.16, simply creates a new rule of evidence stating that: "In a prosecution under this chapter, computer print-outs 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."

In Canada, an Evidence Act (Bill S-33) was introduced to the Senate on 18 November 1982. The bill originated from proposals of the Uniform Law Conference of Canada (1981) and included provisions relevant to the admissibility of computer print-outs and other computer-generated evidence in judicial proceedings. However, the bill was never passed by Parliament. In 1986, a new Canada Evidence Act 1986 was drafted for consultative purposes but has not yet been introduced to Parliament. Section 121 of the bill provides that: "The proponent of a record produced by a computer system may establish that it is an original by:

a. evidence that, on comparison, the record produced by the computer system corresponds in every material particular to the data supplied to that system; or

b. evidence that the computer program used by the computer system to produce the record reliably processes data of the type in question

and that there is no reasonable ground to believe that the record does not correspond in every material particular to the data supplied to the computer system."

On the international level, with respect to laws requiring proof for business transactions, the Committee of Ministers adopted Recommendation No. R (81) 20 concerning the harmonisation of laws relating to the requirement of written proof and to the admissibility of reproductions of documents and recordings on computers. Article 5 of the recommendation enumerates specific requirements which have to be fulfilled if documents are generated by computer systems. In addition, the use of computer-readable data as evidence in court proceedings was discussed by the United Nations Commission on International Trade Law (UNCITRAL) and by the Customs Co-operation Council (CCC). In June 1985, UNCITRAL adopted a recommendation which urges governments to review the legal rules affecting the use of computer records as evidence in litigation, in order to eliminate unnecessary obstacles preventing their admission.

Such international harmonisation of the law of evidence is also desirable for criminal proceedings and mutual assistance, since reproductions or recordings made in one country are increasingly presented as evidence in another country.

5. *Conclusions*

The investigation of computer crime as well as general investigations in computerised environments create new computer-specific problems, especially with respect to the coercive powers of entry and search of premises, the powers of seizure, the duty of witnesses to testify, the duty of witnesses to hand over evidence, the powers of wiretapping as well as the legality of gathering, storing and linking personal data. In most countries, it is unclear how far the traditional coercive powers can be applied and suffice for effective investigations in computerised environments. It is also unclear to what extent civil liberties of citizens must be protected against the storage of personal data in police files by (parliamentary) law. In addition, in common-law countries there are specific legal problems related to the admissibility of computer data in trial process.

A more detailed examination and harmonisation, especially of the coercive powers of investigation authorities, are desirable mainly for two reasons: firstly, the law of criminal procedure should remain the Magna Charta protecting civil liberties of suspects and witnesses; an analogous interpretation of coercive powers could not only infringe on civil liberties

but also the principle of separation of powers, according to which parliament has to decide on new coercive powers and infringements of civil liberties in criminal proceedings. Secondly, a harmonisation of the various national coercive powers would be an important factor for the smooth functioning of international instruments of mutual assistance, since a requested state can only carry out measures admissible to its law.

Consequently, the committee recommends that, in the future, consideration should be given to these 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, a harmonisation of coercive powers and of the respective legal safeguards would promote international legal co-operation in all fields.

IV. International aspects

1. *Introduction*

Computer-related criminality involving a transfrontier situation is becoming increasingly important. Because of the nature of computers, there is increasing potential for storing, moving, using and manipulating data by contact from long range, and the ability to communicate and to transmit rapidly large quantities of data between computer systems over a long distance. As a consequence, the number of places and countries involved in cases of computer crime may increase. The offence may be committed partly in one jurisdiction and partly in another, or even partly in a third one, initiated from practically any place in the world. Obstacles such as distance, border control or necessity of physical presence are no longer relevant. The speed with which a computer-related offence is committed, the volume of data or the sums of money involved and the distance from which the offence is committed present a large difference in comparison to traditional crime. Examples of such criminality have been mentioned above (see I.1). Experts consider international data networks as being vulnerable to computer-related crime, in the banking sector for example. That international business is especially vulnerable has also been recognised by the business community itself (see the ICC report).

In such cases of computer-related crimes with a transfrontier character, the committee considers it necessary for member states to review the existing criteria for determining where the crime has been committed and which jurisdiction is involved in the investigation and prosecution. If more than one state is competent, conflicts of jurisdiction may arise. In addition, in the process of investigating such crimes, it may be necessary

to follow the traces, especially of stored data, abroad and to increasingly use the international instruments of mutual legal assistance. In the light of the transfrontier situation, one has to ascertain whether these instruments, especially the relevant European conventions, can be applied without difficulty.

2. *Problems of jurisdiction connected with the transfrontier character of computer-related crime*

a. *The territoriality principle and extraterritorial jurisdiction*

The authority of a state to establish jurisdiction over acts that take place in its territory is uncontested. However, the interpretation and application of this principle give rise to questions whose answers appear to vary. Such questions relate to the method of determining where an offence has been committed and to the implications of extraterritorial elements.

Many member states determine the place of commission on the basis of what is known as the doctrine of ubiquity, that is, an offence as a whole may be considered to have been committed in the place where a part of it has been committed. It is quite possible that several states consider themselves empowered on the basis of the territoriality principle to take cognisance of the same offence. According to one doctrine, an offence may be considered to have been committed in the place where the consequences or effects of the offence became manifest. This doctrine of effects is accepted in several member states (see the report by the Select Committee of Experts on Extraterritorial Jurisdiction, CDPC, 1990). The area of computer-related crime is of special relevance in this respect.

Today, it is technically possible to manipulate a keyboard in country A, thereby altering data stocked in country B, which are then transferred to country C and there obtain a fraudulent result, for example payment. In respect of damage to computer data or programs or computer sabotage, a "computer virus" could be fed into the computer program in one state, the program containing the virus could be copied hundreds of times and transferred to a number of states. When the virus has damaged or destroyed the program, the effects could manifest themselves in many states. The question then arises of what criteria should apply in order to determine which country should have jurisdiction to investigate and prosecute such offences? Is it the state where the physical manipuulation was committed, the state where the data were altered, the state where the effect was produced, where the offender was physically present, where

the victim is or where the evidence is most easily gathered? Other solutions are also possible. In addition, technical questions come into play, perhaps to a greater extent than for other types of international crimes. It may, for example, be technically impossible to determine in what country the data were located when they were manipulated. It may also often be that the international vehiculation of the data involves so many countries (for example in respect of SWIFT messages within the international banking system), that the place where the offence manifests itself for the first time is the result of fortuitous circumstances. In these cases, the help of data-processing experts is needed to determine where an incident occurs in technical terms and how it affects the system and its functioning.

A wide application of the doctrine of ubiquity leads to the result that a computer-related crime is committed where one of its elements takes place. The international tendency to apply the doctrine of ubiquity can also be seen in the United Kingdom, where a proposal has been made to extend a restricted application of the territoriality principle (see the English report and the solution in Victoria, Australia).

As the examples show, the special nature of transfrontier computer-related crime means that several jurisdictions are involved in the investigation and the prosecution of the offence. It is obvious that positive conflicts of jurisdiction may occur in such cases. There would be a need to co-ordinate the investigation, prosecution and punishment of the offence (or offences in cases where the act may be considered, in some jurisdictions, to constitute several offences).

Another basis for taking jurisdiction, in cases involving extraterritorial elements, are the seven categories of extraterritorial jurisdiction in Chapter II of the report identified by the experts on extraterritorial jurisdiction. Among these categories, it is especially the principle of protection which seems to be particularly relevant for certain types of computer-related offences. These include damaging sensitive government or military data or computer sabotage affecting computer systems of fundamental importance for the functioning of state activities related to its essential interests.

Some states show a trend towards extending their extraterritorial jurisdiction to protect their economic interests. Instances where such interests arise constitute an important part of the transnational data-flow. It is

doubtful whether economic interests are covered by the notion of "essential interests" which could render legitimate extraterritorial jurisdictional claims under the principle of protection (see the report by the experts on extraterritorial jurisdiction).

The report on extraterritorial jurisdiction contains an analysis of different mechanisms to control conflicts of jurisdiction, unilateral, bilateral or multilateral. The solutions and considerations presented by the experts also apply to computer-related crime.

b. *The harmonisation of substantive criminal law*

Of the multilateral mechanisms to control conflicts of jurisdiction, the Select Committee of Experts on Extraterritorial Jurisdiction (PC-R-CC) mentions, *inter alia*, harmonisation of legislation, transfer of proceedings and mutual assistance in criminal matters. The PC-R-CC has previously in the report observed that a certain degree of harmonisation in respect of computer-related crime has already been achieved, probably to a great extent thanks to the work already carried out by OECD and the Council of Europe. It is hoped that the guidelines for the national legislatures will continue the harmonisation process among the member states of the Council of Europe and other states. The committee proposes that the CDPC, in a few years' time, undertake a study of the level of harmonisation in respect of computer-related crime and assess the need for further harmonisation. Should the study reveal such a need, the CDPC might consider the setting up of a committee to draft a convention with a view to harmonising substantive penal law in the area of computer-related crime. One of the advantages of drafting a convention is that states other than the member states of the Council of Europe could be invited to accede to it. This would possibly avoid the creation of so-called "computer-crime havens" and ease the requirement of double criminality whenever this is a condition for international co-operation.

In respect of the other above-mentioned mechanisms, it is, according to the terms of reference, incumbent upon the committee to ascertain whether the European penal conventions are sufficient to fight computer crime at international level and, if not, to propose solutions to remedy this (see 3, *infra*).

c. *The problem of "direct penetration"*

The committee has discussed one further problem. The new technology makes it possible for data to be technically available on line in one

state, while being stored in another state. Such situations may more and more occur in the context of increasing international networks, in particular in a multinational corporate environment. Circumstances of urgency in view of procuring or preserving evidence may require that such data are immediately made available for the purpose of criminal investigation. Elements such as the speed of data communication can easily be used by the person under investigation to make the use of these data as evidence impossible (for example, through erasure, alteration, suppression, etc.). On the other hand, the question has been raised of the legitimacy of a direct online access by the authorities of the investigating state into data bases located in other states and which are not open to the public. Specifically, misgivings were expressed as to whether the direct access has to be seen as an intrusion into the sovereignty of the state of storage. In this case, the more lengthy procedure of the letter rogatory has to be followed, which might, however, jeopardise quick and efficient investigation. Another example, where such misgivings were expressed, is the case where a person is compelled by a court or a prosecutor to generate data which are located in another state but accessible in the state where the investigation is taking place. It is probable, though not certain, that such a measure would go beyond the limits of international law, at least in cases where it would subject the person concerned to conflicting legal requirements.

With regard to the question of "pure" direct penetration, a number of cases could be distinguished, among them:

1. When the police search premises and find a terminal where the screen shows data which are stored abroad;

2. When the police search premises, find a terminal and undertake a search not knowing that the data are stored abroad;

3. When the police search premises, find a terminal and undertake a search, knowing that the data are stored abroad;

4. When the police use their own terminals to access data, knowing that the data are stored abroad.

The first case does not seem to present a specific problem. The data are immediately accessible. No difference in treatment should be accorded to this kind of data.

Opinions might vary concerning the other cases. Some would consider that case No. 2 would constitute a violation of international law regardless of the knowledge of the individual policeman. Others might argue that no such violation is at hand since the policeman was in good

faith. In the latter case, the data could also be used as evidence in the courts of the investigating state. If the case is considered as a violation of international law, whether the evidence could be used by the courts is not clear today.

Cases Nos. 3 and 4 seem to be more evident. In such cases, and in the absence of a specific agreement between the states concerned, the police would probably not have the power of direct penetration. They should then remit to the international instruments of legal co-operation.

The committee has given thoughtful consideration to the question of whether the "direct penetration", which *a priori* does not fall under the European Convention on Mutual Assistance in Criminal Matters, could be made justifiable in exceptional circumstances and under very stringent conditions. Such conditions would be, for example:

– that it would be used only for the taking of measures destined to preserve the *status quo*, that is, so that the data cannot be tampered with;

– that the data would not be used unless the involved state gives its consent;

– that the nature or seriousness of the offence justifies the penetration;

– that there is a strong presumption that the time needed for resorting to a traditional procedure of letters rogatory would compromise the search for truth;

– that the investigating authorities inform the authorities of the other state.

The committee has, however, considered that the time is not ripe for putting forward such a proposal both for reasons of principle and also because of practical considerations. In general, search and seizure and other coercive measures within the territory of another state are illicit unless expressly legitimated under international law (see the report by the experts on extraterritorial jurisdiction). It is unclear whether the direct penetration would constitute such a coercive measure. The question of direct penetration may affect the principle of sovereignty and may constitute an infringement of the exclusive right of the judicial authorities to carry out investigations in their own national territory. It does not seem appropriate that those two important principles of international law should be questioned in this limited context, especially since no need for it seems to have arisen so far. Should such a need emerge in the future, the committee is confident that the Council of Europe will take immediate and efficient action to counter the problem.

3. *The applicability of the European penal law conventions to computer-related crime*

a. *The European Convention on Extradition*

Article 2 of the convention requires that the offence shall be punishable under the laws of both the requesting and the requested Party (the condition of double criminality) and that the offence in question must be subject to deprivation of liberty or a detention order for a maximum period of at least one year or punishment awarded for a period of at least four months (the condition of penalty level, which is of importance in some countries).

Both these conditions may give rise to problems in the context of computer crime. The first requires sufficiently harmonised substantive penal laws, which is not yet the case in the member states of the Council of Europe, even if a certain level of harmonisation has been achieved. As the committee has stated previously, a consensus on definitions of crime, or at least on some constitutive elements, seems desirable in order to ensure that international co-operation becomes possible and that "computer-crime havens" are not created.

The second condition does not always seem evident in respect of certain computer-related criminality, for example the unauthorised access to a computer system or network or the interception of messages to, from and within a computer system or network. The English Law Commission, for example, proposes provisionally that, if hacking is made a criminal offence, it should only be triable in the magistrates' court and not punishable by imprisonment, that is incur only a fine not exceeding the statutory maximum (at present £2 000). Greece has, in this respect, developed a differentiated approach. The act of unauthorised access to data stored in a computer is only punishable by imprisonment not exceeding three months or by a limited fine (Section 370.C of the Penal Code). If, however, the act affects "international relations" or the security of the state, the act is punishable according to another section which provides for higher penalties.

Article 7 gives a Party to the convention the possibility of refusing extradition claimed for an offence which is regarded by its law as having

been committed in whole or in part in its territory. The committee has previously underlined the difficulties that, due to technical circumstances, may arise when determining the place of commission of certain computer offences. If such cases should arise, it is hoped that the countries involved will make a joint effort to find a solution to possible conflicts of jurisdiction.

Other provisions of the convention do not seem to present any computer-specific difficulties other than the ones previously indicated (see, however, Chapter III under item 4). It can, however, be mentioned that the place of the commission of the offence is also relevant, in relation, for example, to the content of the request for extradition (Article 12, paragraph 2.*b*) and in the case of conflicting requests (Article 17). The committee does not foresee any problems in respect of the practical application of these provisions other than in exceptional cases, which could be solved by mutual understanding and consultations between the interested parties.

b. *The European Convention on the Transfer of Proceedings in Criminal Matters*

This convention aims at resolving problems in connection with competing jurisdictional claims (positive conflicts of jurisdiction). As has been observed by the Select Committee of Experts on Extraterritorial Jurisdiction, relatively little use has been made of this form of international legal assistance, even within Europe (only seven states have ratified the convention, opened for signature in 1972). It is the hope of the committee that this form of legal assistance will be explored further in the field of computer-related crime.

With respect to the substantive provisions of the convention, it may first be mentioned that this convention is also based on the principle of double criminality which, in its turn, implies a certain level of harmonisation of substantive penal law. The remarks made in relation to the Extradition Convention are thus equally valid for this convention (see Article 7).

The committee would like to recall the provisions of Article 8, paragraph 1.*e*, which provide for the possibility of the transfer of proceedings in the interests of arriving at the truth and, in particular, where the most important items of evidence are located in the requested state. It may typically be that, in respect of international computer-related crime, this condition is fulfilled.

The place of commission of the offence is again of importance in respect of the application of the right of refusal contained in Article 11, paragraph *h*.

The importance of harmonising substantive penal law is again realised, when studying Article 30, paragraph 1, which refers to "the same offence" (*les mêmes faits*), a provision that gave rise to some discussion when the convention was elaborated, especially in respect of so-called continuing offences (*infractions continues*). The continued falsification of cheques in several countries was cited as an example. It seems that the same misgivings could be expressed for certain hacking offences when several countries are involved.

When similar offences are committed in several countries, for example the unauthorised access into different computer systems, Article 32 of the convention will apply. This requires, however, that a certain level of harmonisation has been reached between the states involved. The same is true for the application of the principle of *ne bis in idem* in Articles 35 and 36 of the convention.

c. *The European Convention on Mutual Assistance in Criminal Matters*

Under Article 2, paragraph *b*, of the convention, mutual assistance may be refused if the execution of the request is likely to prejudice the essential interests of the requested party.

Concern has been voiced in the committee that the Contracting Parties to the convention might extend this notion in respect of requests relating to computer-related crime, which are, for instance, predominantly relative to financial data or concern protected privacy information of its nationals. This may result in a restriction of the practical application of the convention.

A different problem arises in respect of the practical execution of letters rogatory, when states are faced with investigations in connection with the new technology. Article 3 of the convention requires that the execution of letters rogatory should be "for the purpose of procuring evidence or transmitting articles to be produced in evidence, records or documents". It is probable, even if no cases are known yet, that certain countries may have difficulties in searching for information stored on data carriers or seizing such information because of the intangible nature of the requested data. Recommendation No. R (85) 10 of the Committee of

Ministers concerning the practical application of the European Convention on Mutual Assistance in Criminal Matters in respect of letters rogatory for the interception of telecommunications is not applicable in the case of interceptions to, from or within a computer system or network.

Consideration should, in these cases, be given to the importance of the potential interests which could be involved. The requested data may belong to the privacy sphere of an individual or be part of a collection of important business data. Since enormous amounts of data can be stored on one single disc or another type of data carrier, it seems that there is a risk that the requesting party may get access to vast amounts of surplus information. The requesting party may only need information corresponding to one thousand characters but it might, for technical reasons, be necessary to have access to one million characters.

These and other potential problems have led the committee to consider a proposal for elaborating a formal recommendation to clarify the convention in respect of letters rogatory for the selection and collection of computer data, especially in relation to Articles 3 and 14 of the convention. Since no practical experience has yet been gained in this field and in view of the possibly limited application of such a recommendation, the committee has, however, found it appropriate not to propose at this stage the adoption of a formal recommendation. If further experience is gained at a later stage, the CDPC could revert to the question. In the context of such future work, the following items could be studied and possibly proposed:

— Concerning grounds for refusal

i. If, according to the law of the requested party, the nature or gravity of the offence, the status of the person to whom the data relate or who is in possession of, or owner of, or responsible for the computer system or the nature of the data does not permit the use of the investigatory act;

ii. If, in view of the circumstances of the case, such an investigatory act would not be justified according to the law of the requested party governing such acts in that state.

— Concerning the contents of requests for assistance

i. A description, as precise as possible, of the system and programs involved;

ii. In the case of an interception of the communications to, from or within a computer system or network, an indication why the purpose of the request cannot be adequately achieved by other means of investigation;

iii. An indication that the investigatory act has been authorised by the competent authority of the requesting party;

iv. The most precise possible particulars of the data sought.

— Concerning the conditions for the execution of letters rogatory

i. That the judicial authorities of the requested party may exclude those data which, in view of the object and reason of the request, cannot be of any relevance to the criminal proceedings in respect of which the request has been made, before transmitting the data selected and collected to the requesting party;

ii. That the judicial authorities of the requesting party shall as soon as possible destroy or restore, as appropriate, those data transmitted which are of no relevance to the criminal proceedings in respect of which the request has been made and, if the data have been destroyed, shall transmit a copy of the report on the destruction to the requested party;

iii. That, after the investigatory act has taken place, the authorities of the requested party will, in accordance with the law and practice of that party, so inform the person who is in possession of/the owner of/responsible for the system or any other person concerned, that the system has been the subject of such an investigatory act, mentioning the data selected and collected;

iv. That the evidence selected and collected will not be used by the authorities of the requesting party for purposes other than those underlying the letters rogatory in respect of which assistance has been granted, except for cases when the requested party consents.

Other articles of the convention do not call for any comment other than the ones made earlier in respect of the two previously mentioned conventions. Thus, the question of harmonising substantive law is important also in the context of the Mutual Assistance Convention, since the condition of double criminality exists for the execution of letters rogatory for search and seizure (Article 5, paragraph 1.*a*), the level of penalties is equally important in some countries (Article 5, paragraph 1.*b*) and the convention speaks of "property", "records" and "documents" which may

in certain states cause problems because of the intangible nature of computerised information (Article 6). The committee is, in these cases, of the opinion that the parties to the convention should look to the purpose of the convention rather than make a close literal interpretation of it if cases arise in the future, and also solve problems through mutual consultations.

Since the convention, in Article 13, makes special reference to the information relating to judicial records, the committee does not find that the application of the new technology presents any problem in the application of this article.

Article 22 of the convention may finally be noted. It is possible that states in the future, perhaps on the basis of bilateral treaties, may give access to their respective judicial records which often are computerised. Article 22 does not seem to hinder such international co-operation.

d. *Other conventions*

The other European penal law conventions do not seem to present any specific problems related to computer crime other than those discussed above (dual criminal liability, harmonisation of the offences, penalty levels, etc.). It may, however, be noted that the European Convention on the Suppression of Terrorism does not mention any type of computer-related crime as an offence which, for the purposes of extradition, should not be regarded as a political offence (Article 1 of the convention). This convention mentions as offences kidnapping, taking of hostages and serious unlawful detention. Unbelievable as it may seem, cases are reported to have occurred where computers have been taken as "hostages" or in some way have been involved in serous acts of sabotage etc. During a conference on computer crime in Rome 1986, it was claimed that more than sixty cases of serious acts of terrorism had been committed against computers or computer centres. In the view of the committee, Article 2, paragraph 2, of the convention can seldom be resorted to, as it requires an act against property creating a collective danger for persons, for example an explosion of a nuclear installation or the destruction of a dam.

V. Other aspects of computer-related crime

1. *Introduction*

In this final chapter, the committee will discuss certain other aspects of computer-related crime, without however purporting to have treated these aspects in depth. They concern:

i. Security and prevention measures (Section 2 of this chapter), where the committee emphasises the need to take such measures also from a criminological point of view;

ii. Victimisation (Section 3), where the committee points out certain solutions to the problem of the "dark figure", without however recommending one in particular;

iii. Computer-related infringements of privacy (Section 4), where the committee recommends that further work be undertaken in this field within the framework of the Council of Europe.

2. *Security and prevention measures*

The malfunctioning or misuse of computer systems, for instance by the non-availability of information, or its incomplete or erroneous presentation, may have very serious repercussions involving, for example, financial loss, fatal accidents or even the death of patients whose treatment depends on computer assistance. Serious damage may also result from the divulgation of restricted or confidential information about companies, public organisations and individuals and from accidental or fraudulent reading of files and data bases. Damage may take the form of loss of confidence or of standing; it may paralyse an entire business activity and lead to economic ruin, to say nothing of what the consequences might be at national level if financial, political or military secrets were to be spied out, divulged or destroyed, for example by a natural disaster, destroyed material, human failure or intent.

These introductory remarks remind us not only to use criminal law as a protective measure but above all to develop concepts of computer security. It is of the utmost importance that security issues are discussed and treated in a serious manner at all levels and within different types of entities and organisations even if computer security is, first and foremost, a specialised concept in the general field of security in public and private organisations and industry. The committee is only concerned with computer-related crime, but it must be pointed out that "computer security" is a much broader concept, sometimes referred to as "information security". Existing standards such as the ISO/DIS 7498-2, Security Architecture have to be taken into account. These standards include also some valuable background information on security and definitions of important terms and concepts.

For the purpose of the committee's discussions, the following working definition of means of computer security was used:

"Any kind of action or means deployed by the management of a computerised organisation to prevent, detect, withstand or react to attacks on and threats to the free and exclusive availability of a system or its undisturbed functioning or on its integrity and its confidentiality, seeking to balance the cost of the security measure against the desired degree of reduction of the risk."

This definition covers not only actions but also omissions, material as well as non-material means (for example, alarms, measuring instruments, computer programs, patents), personnel (security staff) and formal means (insurance contracts and, in general, all legal and organisational security arrangements).

The definition embraces a range of undesirable situations of both internal and external origin, whether accidental or intentional, which may affect the hardware or software and its users and which may cause damage, operating losses or other types of losses (such as loss of confidence). It describes the importance of having a computer system which is accessible and operational on demand, and able to produce information and perform operations accurately and completely, and maintain the quality of data over a period of time.

Most importantly, the definition indicates the importance that must be accorded to the cost of security. It is virtually impossible to reach an absolute level of security whatever the sum invested, given that there will always be latent and unforeseen risks. Even the most sophisticated security system is not proof against major natural disasters or persons with sufficient motivation, resources and ingenuity, as is shown by the recent intrusion into the NASA computer system by some skilful German hackers who had discovered a flaw in the computer system used. It is also true that most systems are vulnerable against attacks from "insiders", that is persons who work for the company or organisation. As has been shown by researchers, many computer-related crimes are committed by such "insiders".

The cost of security varies, of course, greatly depending on a variety of factors. It has been estimated that, for certain companies, the cost can be as high as 45% of the total budget for computerisation, with this figure varying according to the size of the company and the level of security required. The committee considers that the best approach to take is to establish the cost of installing a security system as a function of the desired risk reduction. While the taking of a security measure has its cost it will reduce the risk of certain computer incidents in a way which is relatively easy to assess fairly accurately. This type of risk management is

applied in the majority of cases, for example by the computer security consultants working in this field, with the object of minimising possible future losses at a reasonable cost. The committee considers it important that concerned organisations and entities review their computer systems and their functioning. This should be done, firstly, by analysing the risks involved, both in general and with respect to special threats that may be posed, given the data stored. The organisation should then decide on the appropriate counter-measures and their implementation. The importance of following up these counter-measures must be stressed, since the degree of risk varies with the lapse of time: perhaps other organisational changes have been made, new devices have come on the market, etc. The importance of training staff with regard to computer security must also be stressed. Making people aware of the risks and the ways by which to counter them is probably the best way of preventing computer-related crime.

One example of a system used by managers to determine the level of security which is necessary for the organisation is the so-called "quantitative risk analysis". Basically, this system tries to assess the rate at which threat events happen, if the system is vulnerable to such threats and the loss that will be experienced if the threat actually occurs. It seems to the committee that this way of assessing the level of reasonable security is rational and the committee recommends that it, or similar systems, be used in all instances where appropriate, depending on, for example, the type and size of the organisation or entity and the information stored in the system.

Apart from giving attention to private initiatives such as risk analysis, it is also necessary for member states of the Council of Europe to engage in steps to improve computer security and prevention. The member states could, apart from providing facilities for training the people concerned, such as teachers, officials and policemen, also establish a legal framework which would require manufacturers and users to observe at least a minimum of regulations relating to computer security. An incentive to take security measures would be the adoption of a provision on the lines suggested by the committee in respect of the unauthorised access to a computer system or network by infringing security measures (offence I.e on the minimum list, see Appendix I of the report). Another example is the requirement, where appropriate, in administrative regulations, for example, that chartered accountants must have adequate training in questions of computer security. A third example is the requirement that certain key officials should have such training. The committee observes in this respect that the taking of security measures is primarily a question for the

company or organisation involved. This does not exclude the government from intervening or, at least, encouraging the introduction of security measures where there are overriding interests demanding state intervention, such as where third party rights need to be protected. Article 7 of the European Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (European Treaty Series, No. 108), ratified by eight member states of the Council of Europe and signed by another ten states, requires, for example, that appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination. The government must of course also protect data which itself holds in the same manner as a private entity. The German Federal Data Protection Act contains, *inter alia*, for these cases a list of security measures to be taken. The Dutch committee considered that the supervisory authority, where such authorities exist (for example in the field of banking, insurance or hospital sector), was entitled to prescribe appropriate security measures.

Yet another example of involvement by the state in questions of computer security is the proposal by the Dutch Committee on Computer Crime. This committee proposes as a guideline for new legislation that a statement regarding the reliability and continuity of the computerised data processing would be included by the directors in the company's annual report; this statement would be assessed by the accountant. The PC-R-CC is not prepared to recommend the introduction of this legislative measure in all member states, but it considers the proposal, as well as other proposals by the Dutch committee, worth discussing by the member states as one way of improving computer security.

These examples of possible measures by the state to improve computer security do not purport to be exhaustive. They show merely that this question is of great concern to the committee as well as the following item on victimisation.

3. *Computer-related victimisation*

The Council of Europe has, in recent years, placed great emphasis on the position of the victim. The 1982 European Convention on the Compensation of Victims of Violent Crimes (European Treaty Series, No. 116), ratified by four member states and signed by another six member states, can be regarded as a milestone for the victim movement in Western Europe. The Sixteenth Criminological Research Conference, in 1984, was

entirely devoted to research on victimisation (see CDPC, *Collected Studies in Criminological Research*, Volume XXIII, Strasbourg, 1985). The Select Committee of Experts on the Victim and Criminal and Social Policy elaborated Recommendation No. R (85) 11 on the position of the victim in the framework of criminal law and procedure, adopted by the Committee of Ministers in June 1985, as well as Recommendation No. R (87) 21 on assistance to victims and the prevention of victimisation, adopted by the Committee of Ministers in September 1987.

Questions of computer-related victimisation have, in particular, been dealt with at the 7th United Nations Congress for the Prevention of Crime and the Treatment of Offenders in 1985 and during its preparatory work. Particular interest has been given to the right to obtain rectification or erasure of personal data, processed contrary to Articles 5 and 6 of the aforementioned Data Protection Convention, and give the victims the possibility of applying for compensation (see, for example, Article 10 of the Data Protection Convention). The fact that computer-related crime can affect many people and cost large sums of money has also been mentioned as a particular feature of this type of crime.

Research into computer-related crime in several countries has shown that most of the victims are to be found in the banking or insurance sector and in government organisations and entities. It has been observed that the victims of such crimes, in particular in the financial sector, are reluctant to report the crime, thus leading to the assumption that the dark figure (unreported crimes vs. reported ones) is probably very high.

It is clear that the co-operation of the victim is an essential factor in suppressing computer-related crimes. Reluctance to report, therefore, constitutes a serious problem in the fight against such crimes. In many cases, only information laid by the victim opens up the possibility of investigating the crime and catching the offender and, where he is known, prosecuting him. Revealing computer crimes to the police and other appropriate authorities and to society at large can have advantages for data-processing institutions on the level of prevention. It may lead to a more accurate assessment of shortcomings and risks in the victim's firm or other organisations in the same sector and, as a consequence, to an improvement in the quality of security measures and the means of detecting such crimes. It may broaden the knowledge and experience of police, prosecutors and courts. It is even asserted that non-disclosure "encourages other wrongdoers to have a go" (Scottish report, p. 22). In the opinion of renowned researchers, a number of computer crimes could

have been avoided or detected earlier, if more information about *modi operandi* had been made available thanks to a greater willingness of the victims to report crimes.

Victims' reluctance to report computer-related crimes is, on the other hand, not irrational; there are several reasons which put a brake on their reaction. Such factors are, for instance, fear that the public might lose confidence in the institution and that the resulting economic losses would probably far exceed those caused by the crime itself; the management's fear of losing face as a result of the publicity; disadvantages related to the conduct of proceedings (too long, causes loss of time for the management, etc.); the victims' perception or lack of knowledge and reluctance on the part of the authorities to investigate the crime, etc. (see the Dutch and Scottish reports).

The committee has discussed several ways of obtaining the co-operation of the victim. The most radical solution would be to oblige by law the managers of organisations to report to the police any illegal act committed within their EDP networks; failure to lodge a complaint would be considered an offence of varying seriousness, depending on the nature of the organisation's activity. The committee has rejected this solution as being contrary to the legal traditions of several states. The custom has been to leave it to the victim to decide whether he wants to involve the organs of criminal justice or not, and whether for example he wants to deal with the damage himself by asking the offender to pay damages and, where it is an offence by an insider, possibly also terminating the employment relationship. This sort of approach is also in harmony with the subsidiary role of the criminal law and reduces the workload of the prosecuting agencies. If the reporting of offences was made obligatory, the victim would also have the feeling in many cases of being forced to play the part of assistant to the police or prosecuting service. Finally, compulsory reporting would lead to an imbalance with regard to other offences where the computer plays no part and where such a duty does not exist. In addition, the committee has serious doubts about how such a duty should be enforced in practice if the loss itself is concealed, and whether it is appropriate to impose criminal penalties on the victim for failure to disclose an incident of computer crime (see the Dutch and Scottish reports).

A less stringent solution would be to introduce an obligation of disclosure not to the police, but at least in certain cases to a specialised body, especially a supervisory one. Such a body would then act as an intermediary *vis-à-vis* the judicial authority and assess the case (see the Dutch report). In some countries, such a duty exists. The Bank Protection

Act in the United States and other provisions require banks to report all frauds and inexplicable losses of more than US$ 1 000 to the banking authorities; severe sanctions are imposed for any failure or delay in reporting such acts. A special questionnaire, to be sent to the Federal Deposit Insurance Corporation, is mandatory in the case of fraud involving electronic fund transfer systems. The example given shows that such a duty cannot be introduced for all computer-related crimes and for all victims. As mentioned above and confirmed by United States law, it cannot be restricted to cases of computer-related crimes. The feasibility of such a solution is dependent on the use and structure of control systems in related areas in a member state. It also depends on general policy as regards the involvement and the obligations of enterprises concerned as victims. Some of the counter-arguments against a duty of disclosure to the prosecuting authorities are valid here, too, and may lead to the same conclusion. The committee, therefore, does not make a recommendation, but it is a point which in some instances may be considered by a member state.

A more subtle reporting system has been discussed in the Netherlands, as proposed by the Dutch Committee on Computer-Related Crime. A "platform" could be established, where discussion and exchange of views based on cases of computer crime (with no names disclosed) take place between actual or potential victims and law enforcement agencies. The platform's function could also be to collect cases so that companies, organisations and the public can obtain a better understanding of the risks, shortcomings in the systems, etc.

Other solutions were also discussed by the committee. One would be to make a special security certificate mandatory for EDP systems, at least for large and medium-sized ones. This certificate would be awarded after verification by a special corps of auditors and after a regular check on the efficiency of these measures. Auditors would then have to report crimes discovered in the exercise of their office. This solution was, however, rejected by the committee as being contrary to the legal traditions of several member states and the role of the auditor.

Lastly, in order to indirectly encourage victims to report offences, the committee discussed whether managers of EDP systems should be obliged by law to take out insurance cover. Reporting the crime to the authorities would naturally be the condition for claiming compensation from the insurance company. The committee, however, also rejected this solution since it found that the situation was not comparable to existing compulsory insurances.

4. *Computer-related infringements of privacy, general principles*

The aforementioned Data Protection Convention contains, in its Article 10, a provision stating that "Each Party undertakes to establish appropriate sanctions and remedies for violations of... the basic principles for data protection...".

This article is to be understood in such a way that the duties of the data users and the rights of the data subjects should be reflected in the national legislation of member states by corresponding sanctions and remedies. It was, however, left to such states to determine the nature of these sanctions and remedies (civil, administrative, criminal).

A comparative analysis of the various laws enacted or planned in the member states shows that a certain uniformity in the general administrative and civil regulations of the privacy laws has been achieved. However, considerable differences remain in general administrative and civil regulations. They are due to several factors, such as the legislative rationale and different legal traditions of member states. They may, for instance, concern differences in scope of application, data covered by the law, manually recorded data, formal requirements for starting data processing, public authorisation, control institutions, etc. These differences are not only relevant for administrative law, but to a large extent they also determine differences in criminal law which often refers to the administrative regulations.

The Austrian Data Protection Act, the Danish Private Registers Act and the German Federal Data Protection Act, which all punish certain cases of illegal disclosure, dissemination and obtainment of and/or access to data, can be given as examples of the punishment of infringement of substantive privacy rights. Concerning administrative law, the infringement of legal requirements regarding the commencement of personal data processing may be mentioned, for example in the French Act on data processing, data files and individual liberties and the Danish Act, already referred to. The penalties for these offences vary between member states, if made punishable at all.

The committee has given thoughtful consideration to this state of the law. However, it has limited itself to discussing certain basic principles which should be taken into account by all member states when legislating in the field of computer-related criminal privacy legislation. The committee recommends that further work should be undertaken by appropriate bodies within the Council of Europe or, for example, by the committee set up pursuant to Article 18 of the Data Protection Convention. This work could include ascertaining:

i. what penal and other sanctions against infringements of privacy laws already exist;

ii. court decisions applying these sanctions;

iii. the degree of uniformity between different legislations or lack of uniformity; and

iv. the need and suggestions for international harmonisation, if any.

A problem which needs special attention is the penal law aspects of the direct or indirect control of workers at their workplaces, using automated systems or techniques, often computers (systems to register telephone calls, for example), which might violate the privacy of workers.

The use of such techniques has already encountered strong resistance in some member states (for example, in Italy, France, the Federal Republic of Germany) and led to the intervention of public authorities (see, for example, in Italy the judgments of the criminal court, *Pretura* of Milan). This problem has also been discussed from a different angle in Recommendation No. R (89) 2 of the Committee of Ministers on the protection of personal data used for employment purposes.

The basic principles referred to above and agreed to by the committee are 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. A 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 to incriminate substantive infringements of privacy and adopt a formal approach, based on administrative requirements of notification of potentially harmful data-processing 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-obstacles*), 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 (that is, 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 justice, on complaint of the victim or of the Privacy Protection Commissioner or of the Privacy Protection Authority (principle of complaint).

It is the hope of the committee that the acceptance of these principles will serve as a basis for future work on computer-related infringements of privacy and that they will help establish an adequate criminal law system in the data-processing area.

APPENDIX I

Summary of the guidelines for national legislatures

(This summary should be read in conjunction with Chapter II of the report on pp. 33 to 69. The reader may note that criminal liability should be inflicted for intentional action only, see p. 35, under item 4.)

I. *Minimum list of offences necessary for a uniform criminal policy on legislation concerning computer-related crime*

a. *Computer-related 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 with the intent of procuring an unlawful economic gain for himself or for another person (alternative draft: with the intent to unlawfully deprive that person of his property).

b. *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 which would, according to national law, constitute an offence of forgery if it had been committed with respect to a traditional object of such an offence.

c. *Damage to computer data or computer programs*

The erasure, damaging, deterioration or suppression of computer data or computer programs without right.

d. *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 telecommunications system.

e. *Unauthorised access*

The access without right to a computer system or network by infringing security measures.

f. *Unauthorised interception*

The interception, made without right and by technical means, of communications to, from and within a computer system or network.

g. *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.

h. *Unauthorised reproduction of a topography*

The reproduction without right of a topography, protected by law, of a semiconductor product, or the commercial exploitation or the importation for that purpose, without right, of a topography or of a semiconductor product manufactured by using the topography.

II. *Optional list*

a. *Alteration of computer data or computer programs*

The alteration of computer data or computer programs without right.

b. *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.

c. *Unauthorised use of a computer*

The use of a computer system or network without right, that either:

i. 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

ii. 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

iii. causes loss to the person entitled to use the system or harm to the system or its functioning.

d. *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 oneself or for another person, or to cause harm to the holder of the right.

APPENDIX II

Select international bibliography

Australia

Briscoe, W.G./Law Reform Commission of Tasmania, *Research Paper on Computer Misuse*, Hobart, Tasmania,1984.

Fitzgerald, Kevin J., *The Computer Abuse Profile in Australia*, edited by the Computer Abuse Research Bureau, Chisholm Institute of Technology, Caulfield, Victoria, 1982.

McNiff, Francine/Juris, B., *Criminal Liability for Australian Computer Abuse*, edited by the Computer Abuse Research Bureau, Caulfield Institute of Technology, Melbourne, 1980.

Austria

Jaburek, Walter, "Software für Großsysteme — Ist Computerkriminalität eingeplant?" in Koelsch, Raimund/Schmid, Werner/Schweiggert, Franz, *Wirtschaftsgut Software*, Stuttgart, 1985, p. 83 *et seq.*

Jaburek, Walter/Schmölzer, Gabriele, *Computer-Kriminalität*, Wien 1985.

Justizausschuß des österreichischen Nationalrats: "Bericht des Justizausschusses über den Antrag der Abgeordneten Dr. Ofner und Genossen betreffend ein Strafrechtsänderungsgesetz", 1987 (2/A), in *Nr. 359 der Beilagen zu den Stenographischen Protokollen des Nationalrates*, Volume XVII, GP.

Schmölzer, Gabriele, "Das neue Computer-Strafrecht (Strafrechtsänderungs- Gesetz, 1987)", in *EDV und Recht*, 1988, p. 20 *et seq.*

Zima, Herbert, "Computerkriminalität", in *Journal für Betriebswirtschaft*, 1980, No. 2, p. 82 *et seq.*

Belgium

Cools, Marc/De Houwer, Joke/Erkelens, Catherine/Vanderhoydonck, Francis/ De Schutter, Bart, *Soft-en hard, ware het niet om de fraude Bedenkingen over computercriminaliteit*, 7 JUS Interuniversitaire Studenten Reeks, Antwerpen, 1985.

Erlekens, Catherine, «La délinquance informatique belge et le droit pénal belge», in *Supplément Droit de l'Informatique*, 1985, issue 6, p. 21 *et seq.*

Gutwirth, S., «De beteugeling van informaticafraude. Naar een nieuw informatierecht», in *Rechtskundig Weekblad*, 1985/86, p. 2459 *et seq.*

Schutter, Bart de/Spryt, B., "Computerfraude: De relatjeve onmacht van het interne en het internationale strafrecht", in De Vroede (editor), *Technologie en Recht — Kluwer Rechtswetenschappen*, Antwerpen, 1987, p. 353 *et seq.*

Schutter, Bart de (editor), "Informaticacriminaliteit", in *Kluwer Rechswetenschappen*, Antwerpen, 1988, p. 778 *et seq.*

Spreutels, Jean P., «Infractions liées à l'informatique en droit belge», *Revue de Droit Pénal et de Criminologie*, 1985, p. 357 *et seq.*

Spruyt, B./Schutter, Bart de, "Grensoverschrijdende informaticacriminaliteit", in *Kluwer Rechtswetenschappen*, Antwerpen, 1989, p. 147 *et seq.*

Verstraeten, R., "Diefstal van computergegevens: Revolutie in het strafrecht?", in *Rechtskundig Weekblad*, 1985/86, p. 215 *et seq.*

Canada

Department of Justice, *Response of the Government of Canada to the Report of the Parliamentary Sub-Committee on Computer Crime*, Ottawa, 1983.

Institute of Law Research and Reform of the University of Alberta, background paper on *Improper Interference with Computers and the Misappropriation of Commercial Information*, Edmonton/Alberta, 1983.

Piragoff, Donald K., "Combating crime with criminal laws", in H.W.K. Kaspersen (editor), *Strafrecht in de Informatiemaatschappij*, Amsterdam, 1986, p. 103 *et seq.*

«Les projets législatifs canadiens visant à la protection de l'intégrité des systèmes informatiques», in *Supplément Droit de l'Informatique*, 1986, issue 6, p. 33 *et seq.*

Denmark

Greve, Vagn, *EDB-strafferet*, København, 1986.

Hof, Ulla, "EDB og EDB-Kriminalitet", in *Anklagemyndighedens arsberetning*, København, 1981, p. 58 *et seq.*

Meilby, Finn/Hob, Ulla, "Mandatsvig", *Juristen*, 1985, p. 41 *et seq.*

Federal Republic of Germany

Bschorr, Christian K., *Computer-Kriminalität — Gefahr und Abwehr*, Düsseldorf, Wien, New York, 1987.

Haft, Fritjof, "Zur Situation des Datenschutzstrafrechts", *Neue Juristische Wochenschrift*, 1979, p. 1194 *et seq.*

Lenckner, Theodor, *Computerkriminalität und Vermögensdelikte*, Karlsruhe, 1981.

Lenckner, Theodor/Winkelbauer, Wolfgang, "Computerkriminalität — Möglichkeiten und Grenzen des 2. WiKG", *Computer und Recht*, 1986, p. 483 *et seq.*, 654 *et seq*, 824 *et seq.*

Möhrenschlager, Manfred, "Der Regierungsentwurf eines Zweiten Gesetzes zur Bekämpfung der Wirtschaftskriminalität", *Wistra*, 1982, p. 201 *et seq.*

Richter, Hans Ernst, "Computerkriminalität und Strafrecht", in *Handbuch der modernen Datenverarbeitung — DV-Recht*, Wiesbaden, 1989, Volume 146 (1989), p. 76 *et seq.*

Sieber, Ulrich, *Computerkriminalität und Strafrecht*, 2. edition, Köln, 1980.

Sieber, Ulrich, *Gefahr und Abwehr der Computerkriminalität. Betriebs-Berater*, 1982, p. 1433 *et seq.*

Sieber, Ulrich, *Informationstechnologie und Strafrechtsreform*, Köln, 1985.

Stoll, Clifford, *Kuckucksei — Die Jagd auf die deutschen Hacker, die das Pentagon knackten*, Frankfurt am Main, 1989.

Finland

Kainonaa, Seppo, "Tietoturva sekä vahingot ja väärinkäytökset", *ssa. Titkimus-Raportti 3/84*, edited by the Tietotekiikan Kehittämiskeskus r.y., Helsinki, 1984.

Lehtimaja, Lauri, "Tietokonerikollisuuteen liityviä oikeudellisia ongelmia", in *Defensor Legis*, 1983, p. 54 *et seq.*

"Atk-turvallisuus ja lainsäädänto", in *Suomen Poliisilehti*, 1984, p. 40 *et seq.*

France

Chaigneau, Anne, «La délinquance télématique», in *Télématique et communication — Un nouveau droit*, Actes des Troisièmes Entretiens de Nanterre de Droit de l'Informatique, Paris, 1985, p. 91 *et seq.*

Chamoux, Françoise, «La loi sur la fraude informatique: des nouvelles incriminations», in *La Semaine Juridique*, 1988, I. 3321.

Chamoux, Jean-Pierre, *Menaces sur l'ordinateur*, Paris, 1986.

Croze, Hervé, «L'apport du droit pénal à la théorie générale du droit de l'informatique (à propos de la loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique)», in *La Semaine Juridique*, 1988, I.3333.

Lamy, «Droit de l'informatique», *Les biens informatiques, moyens d'une fraude*, n^{os} 2337 à 2401, Paris, 1988.

Les biens informatiques, objets d'une fraude, n^{os} 2431 à 2500, Paris, 1988.

Pitrat, Charlotte Marie, «Fraude informatique et pouvoirs publics», in *Supplément Droit de l'Informatique*, 1985, issue 6, p. 46 *et seq.*

Pradel, Jean/Feuillard, Christian, «Les infractions commises au moyen de l'ordinateur», *Revue de Droit Pénal et de Criminologie*, 1985, p. 307 *et seq.*

Vivant, Michel, «A propos des biens informationnels», in *La Semaine Juridique*, 1984, I. 3132.

Greece

Stamoulis, Spiridon, «Problems of Liability in Computer Crime», in *NoB*, 1987, p. 1010 *et seq.*

Vassilaki, Irini, «Program Piracy and Article 16 — 17 L. 146/1914», in *NoB*, 1988, p. 1338 *et seq.*

Italy

Picotti, Lorenzo, *Appendice a Criminalità da Computer. Politica del diritto*, 1984, p. 629 *et seq.*

"Problemi penalistici in tema di falsificazione di dati informatici", in *Il diritto dell'informazione e dell'informatica*, 1985, p. 939 *et seq.*

Rodotà, Stefano, "Protezioni dei dati e circolazione dell'informazione", in *Rivista critica del diritto privato*, 1984, p. 721 *et seq.*

Russo, Licia, "Informatica e criminalità", in *Rivista italiana di diritto e procedura penale*, 1984, p. 324 *et seq.*

Sarzana, Carlo, "Note sul diritto penale dell'informatica", in *La giustizia penale*, 1984, Part I, p. 21 *et seq.*

Sarzana, Carlo, «La fraude informatique: remarques sur l'accès illicite à l'ordinateur», in *Informatique et droit: 20 ans d'expérience*, Congrès international organisé par l'ADIJ, Strasbourg, 1987, p. 373 *et seq.*

Japan

National Police Agency, *Report for Investigators of Computer Crime*, Tokio, 1982.

Soyoda, Hisashi, "Das neue Computerstrafrecht in Japan", in *Wistra*, 1988, p. 167 *et seq.*

White Paper on Police, Tokio, 1983.

White Paper on Police, Tokio, 1984.

Luxembourg

Jaeger, Marc, «La fraude informatique», in *Revue de Droit Pénal et de Criminologie*, 1985, p. 323 *et seq.*

Netherlands

Brandenburg, Koos, *Criminalistiek en Computer*, Graduation thesis of the Police Academy of Apeldoorn, 1984.

Dijken, Pieter van, "Computer en criminaliteit", in *Algemeen Politieblad*, 1983, p. 487 *et seq.*

Kaspersen, H.W.K./Keizer, Nico, "Het Nederlandse strafrecht en computermisbruik", in H.W.K. Kaspersen (editor), *Strafrecht in de Informatiemaatschappij*, Amsterdam, 1986, p. 35 *et seq.*

Kaspersen, H.W.K., *Computermisdaad en strafrecht*, Antwerpen, 1986.

Vandenberghe, Guy P.V., "Computermisbruik, beveiliging en strafrecht", in H.W.K. Kaspersen (editor), *Strafrecht in de Informatiemaatschappij*, Amsterdam, 1986, p. 25 *et seq.*

Norway

Andenaes, Johs/Fongner, Else/Bugge, Oug/Thor, Yrigstad/Lasse, Drolsum/Schjolberg, Stein/Selmer, Knut S., *Datakriminalitet. Norges Offentlige Utredninger*, No. 31, Oslo, 1985.

Bjoernstad, Åge/Tjåland, *Computer Crime — Reported and Unreported, Summary — A study of the extent of computer crime in Norway*, edited by the Department of EDP-Auditing, Norwegian School of Management, 1989.

Schjolberg, Stein, *Computers and Penal Legislation*, Oslo, 1983.

Schjolberg, Stein, *Computers and penal legislation — A study on the legal politics of new technology*, Complex 2/83, Oslo, 1983.

Spain

Madrid, Conesa F., *Estudio de Derecho, Informática y derecho penal*, Valencia, 1983.

Morales Prats, Fermín, *La tutela penal de la intimidad: privacy e informática*, Barcelona, 1984.

"Presupposti politico-criminali per una tutela della riservatezza informatica (con particolare riguardo all'ordinamento spagnolo)", in A. Giuffrè (editor), *Il Diritto dell'informazione e dell'informatica*, Complex 2/86, Milano, 1986.

"Problemática jurídico-penal de las libertades informáticas en España tras diez años de vigencia de la Constitución de 1978", in *Estudios penales y criminológicos*, Volume XII, edited by Universidad de Santiago de Compostela, 1989, p. 305 *et seq.*

Romeo Casabona, Carlos María, *Poder informático y seguridad jurídica — La función tutelar del derecho penal ante las nuevas tecnologías de la información*, Madrid, 1987.

Sweden

Solarz, Artur, *Computer Technology and Computer Crime*, Report No. 8 of the Research and Development Division, edited by the National Council for Crime Prevention, Stockholm, 1981.

Datorteknik och brottslighet, edited by the National Council for Crime Prevention, Stockholm, 1985.

ADB och Brott — Kriminalitetens utveckling i ett informationssamhälle, København, 1987.

Swedish Ministry of Defence, *The Vulnerability of the Computerised Society*, Stockholm, 1979.

Switzerland

Bauknecht, "Computer-Kriminalität", in Neutra Treuhand AG (editor), *Wirtschafskriminalität*, Zürich, 1982, p. 99 *et seq.*

Eidgenössisches Justiz- und Polizeidepartement (editor), *Bericht zum Vorentwurf über die Änderung des Strafgesetzbuches und des Militärstrafgesetzes betr. die strafbaren Handlungen gegen das Vermögen und die Urkundenfälschung*, Bern, 1985.

Fischer, Thomas, "Computer-Kriminalität, Gefahren und Abwehrmaßnahmen", *Betriebswirtschaftliche Mitteilungen*, Volume 71, Bern, 1979.

Rohner, Louis, *Computerkriminalität — Strafrechtliche Probleme bei Zeitdiebstahl und Manipulationen*, Zürich, 1976.

Stratenwerth, Günter, "Computerbetrug", in *Schweizerische Zeitschrift für Strafrecht*, Volume 98 (1981), p. 229 *et seq.*

Zimmerli, Erwin/Liebl, Karlhans (editors), *Computermißbrauch — Computersicherheit*, Ingelheim/Küsnacht, 1984.

Zweifel, Sibylle, *Buchführungsdelikte mittels EDV und Maßnahmen zu deren Verhinderung*, Zürich, 1984.

United Kingdom

McKnight, Gerald, *Computer Crime*, London, 1973.

Norman, Adrian R.D., *Computer Insecurity*, London, 1983.

Scottish Law Commission, *Report on Computer Crime*, edited by Her Majesty's Stationery Office, Edinburgh, 1987.

The Law Commission, *Computer Misuse*, Working Paper No. 110, edited by Her Majesty's Stationery Office, London, 1988.

Wasik, Martin, "Law Reform Proposals on Computer Misuse", in *Criminal Law Review* 1989, p. 257 *et seq.*

"Following in American Footsteps? — Computer Crime Developments in Great Britain and Canada", in *Northern Kentucky Law Review*, Volume 14, 1987, p. 249 *et seq.*

Wong, Ken, *Computer Crime Casebook*, edited by BIS Applied Systems, Manchester, 1983.

Computer-related fraud. Information Age, 1983, p. 16 *et seq.*

Computer-Related Fraud Casebook, edited by BIS Applied Systems, Manchester, 1983.

United States of America

Bequai, August, *Computer Crime*, Massachusetts, 1978.

Bequai, August, *How to Prevent Computer Crime*, Toronto, 1983.

Bloombecker, Jay J., *The Computer Crime Law Reporter*, looseleaf, edited by the National Center for Computer Crime Data, Los Angeles.

"Computer crime update: the view as we exist", 1984, in *Western New England Law Review*, Volume 7 (1985), p. 627 *et seq.*

Couch, Robert, "A Suggested Legislative Approach to the Problem of Computer Crime", *Washington and Lee Law Review*, Volume 38 (1981), p. 1173 *et seq.*

Kraus, Leonard/MacGahan, Aileen, *Computer Fraud and Countermeasures*, Englewood Cliffs, New York, 1979.

McKnight, Gerald, *Computer Crime*, London, 1973.

Parker, Donn B., "Computer Abuse Research Update", *Computer and Law Journal*, Volume 2 (1980), p.329 *et seq.*

Parker, Donn B., *Fighting Computer Crime*, New York, 1983.

Taber, John K., "A Survey of Computer Crime Studies", *Computer and Law Journal*, Volume 2 (1980), p.275 *et seq.*

United States Department of Justice, *Computer Crime — Legislative Resource Manual*, Washington, DC, 1980.

International and comparative studies

Briat, Martine, «La fraude informatique: une approche de droit comparé», in *Revue de droit pénal et de criminologie*, 1985, p.267 *et seq.*

Camera dei Deputati (editor), *Banche Dati e tutela della persona*, 2nd edition, Rome, 1983.

Commission of the European Communities — Information Technology Task Force, *The Vulnerability of the Information-Conscious Society — European Situation*, summarised conclusions, 1984.

ICC (International Chamber of Commerce), *Computer-Related Crime and Criminal Law: an International Business View*, Position paper No. 11, Paris, 1988 (also available in French).

OECD (Organisation for Economic Co-operation and Development) (editor), *Computer-related Criminality: analysis of Legal Policy*, Paris, 1986.

Schutter, Bart de, "Grensoverschrijdende computercriminaliteit — Nood aan harmoniserende aanpak", in H.W.K. Kaspersen (editor), *Strafrecht in de Informatiemaatschappij, Amsterdam*, 1986, p. 143 *et seq.*

Sieber, Ulrich, *The International Handbook on Computer-Crime — Computer-Related Economic Crime and the Infringements of Privacy*, Chichester, 1986.

Sieber, Ulrich, "Legal Protection of Computer Data, Programs and Semiconductor Products: A Comparative Analysis with Suggestions for Legal Policy", in ICC (International Chamber of Commerce), *International Contracts for Sale of Information Services*, Paris, 1988, p. 7 *et seq.*

Sieber, Ulrich, "Collecting and Using Evidence in the Field of Information Technology — A Comparative Analysis", in, Albin Eser/Jonatan Thormundsson (editors), *Old Ways and New Needs in Criminal Legislation*, Freiburg, 1989, p. 203 *et seq.*

Other publications in the same field

Protection of the privacy of individuals vis-à-vis *electronic data banks in the public sector, Resolution (74) 29* (1975), ISBN 92-871-0492-1

Criminological aspects of economic crime (1977), ISBN 92-871-0595-2

Teaching, research and training in the field of "computers and law", Recommendation No. R (80) 3 (1981), ISBN 92-871-0494-8

Regulations for automated medical data banks, Recommendation No. R (81) 1 (1981), ISBN 92-871-0495-6

Economic crime (1981), Recommendation No. R (81) 12, ISBN 92-871-0588-X

Harmonisation of laws relating to the requirement of written proof and to the admissibility of reproductions of documents and recordings on computers, Recommendation No. R (81) 20 (1982), ISBN 92-871-0044-6

Explanatory report on the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (European Treaty Series No. 108) (1981), ISBN 92-871-0482-4

Telephone tapping and the recording of telecommunications in some Council of Europe member states, (1982), ISBN 92-871-0055-1

The protection of users of computerised legal information services, Recommendation No. R (83) 3 (1983), ISBN 92-871-0279-1

Protection of personal data used for scientific research and statistics, Recommendation No. R (83) 10 (1983), ISBN 92-871-0317-8

Letters rogatory for the interception of telecommunications (1985), Recommendation No. R (85) 10, ISBN 92-871-0839-0

Protection of personal data used for the purposes of direct marketing, Recommendation No. R (85) 20 (1986), ISBN 92-871-0876-5

Protection of personal data used for social security purposes, Recommendation No. R (86) 1 (1986) ISBN 92-871-0924-9

Regulating the use of personal data in the police sector, Recommendation No. R (87) 15, ISBN 92-871-1587-7

Computers and law. Study on new technologies: a challenge to privacy protection? ISBN 92-871-1616-2

APPENDIX III

Participants in the Select Committee of Experts on Computer-related Crime

Mr H. Tiegs (Austria),
Mr B. Carlsen (Denmark),
Mr P. Castel, Mr F. Caillet and Mr J.P. Mazon (France),
Mr M. Möhrenschlager (Federal Republic of Germany, Chairman),
Mr D. Spinellis and Mrs I. Vassilaki (Greece),
Mr C. Sarzana (Italy, Vice-Chairman),
Mr M. Jaeger, Mr J.-M. Hary and Mr G. Heisbourg (Luxembourg),
Mr A. Patijn and Mr A.C. Berghuis (the Netherlands),
Mrs R. Noer (Norway),
Mr J.A. Barreiros, Mr A. Raposo and Mr M. Bigotte-Chorao (Portugal),
Mr A. Laguia Arrazola (Spain),
Mr D. Victor (Sweden)
Mr P.-H. Bolle (Switzerland)

Observers

Mr D. Piragoff and Mr G. Lemoine (Canada),
Mr L. Lehtimaja (Finland),
Mr T. Johnson and Mr V. Comras (United States of America),
Mr H. Ueno, Mr H. Yanagezawa, Mr S. Matoba and Mr A. Ito (Japan),
Mr G. Papapavlou (EEC),
Mr H.P. Gassmann, Mr P. Kenneth and Mrs D. Hurley (OECD)
Mr C. Sarzana (UNSDRI)

Scientific experts

Mr B. de Schutter, Miss P. Poelmans (Belgium) and Mr U. Sieber (Federal Republic of Germany)

Mr H.G. Nilsson acted as the committee's secretary.

SALES AGENTS FOR PUBLICATIONS OF THE COUNCIL OF EUROPE

AUSTRALIA
Hunter Publications
58A, Gipps Street
AUS-3066 COLLINGWOOD, Victoria

AUSTRIA
Gerold und Co.
Graben 31
A-1011 VIENNA 1

BELGIUM
La Librairie européenne S.A.
244, rue de la Loi
B-1040 BRUSSELS

CANADA
Renouf Publishing Company Limited
1294 Algoma Road
CDN-OTTAWA ONT K1B 3W8

CYPRUS
MAM
The House of the Cyprus Book
P.O. Box 1722
CY-NICOSIA

DENMARK
Munksgaard
Book and Subscription Service
P.O. Box 2148
DK-1016 COPENHAGEN K

FEDERAL REPUBLIC OF GERMANY
Verlag Dr. Hans Heger
Herderstraße 56
Postfach 20 13 63
D-5300 BONN

FINLAND
Akateeminen Kirjakauppa
Keskuskatu 1
P.O. Box 128
SF-00101 HELSINKI

GREECE
Librairie Kauffmann
28, rue Stadiou
GR-ATHENS 132

ICELAND
Bókabúd Máls og menningar
Laugavegi 18
IS-REYKJAVIK 101

IRELAND
Government Stationery Office
Publications Section
Bishop Street
IRL-DUBLIN 8

ITALY
Libreria Commissionaria Sansoni
Via Benedetto Fortini, 120/10
Casella Postale 552
I-50125 FLORENCE

LUXEMBOURG
Librairie Bourbon
(Imprimerie Saint-Paul)
11, rue Bourbon
L-1249 LUXEMBOURG

MALAYSIA
Library Building
University of Malaya
P.O. Box 1127
Jalan Pantai Baru
59700 KUALA LUMPUR

NETHERLANDS
InOr-publikaties
Noorderwal 38
Postbus 14
NL-7240 BA LOCHEM

NEW ZEALAND
Government Printing Office
Mulgrave Street
(Private Bag)
NZ-WELLINGTON

NORWAY
Akademika, A/S Universitetsbokhandel
P.O. Box 84
Blindern
N-0314 OSLO

PAKISTAN
Tayyab M.S. Commercial Services
P.O. Box 16006
A-2/3, Usman Ghani Road
Manzoor Colony
PAK-KARACHI-44

PORTUGAL
Livraria Portugal
Rua do Carmo, 70
P-1200 LISBON

SPAIN
Mundi-Prensa Libros S.A.
Castelló 37
E-28001 MADRID

Libreria de la Generalitat
Rambla dels Estudis, 118
E-08002 BARCELONA

SRI LANKA
Centre for Curriculum Advancement
78 Eachamottai Road
CL-JAFFNA

SWEDEN
Aktiebolaget C.E. Fritzes
Regeringsgatan 12
Box 163 56
S-10327 STOCKHOLM

SWITZERLAND
Buchhandlung Heinimann & Co.
Kirchgasse 17
CH-8001 ZURICH

Librairie Payot
6, rue Grenus
CH-1211 GENEVA 11

TAIWAN — HONG KONG
SINGAPORE
Mappamundi Taiwan
7 Fl. 258, Nanking E. Rd.
Sec. 3 Taipei
TAIWAN R.O.C.

TURKEY
Librairie Haset Kitapevi A.S.
469, Istiklâl Caddesi
Beyoglu
TR-ISTANBUL

UNITED KINGDOM
HMSO
Agency Section
51 Nine Elms Lane
GB-LONDON SW8 5DR

UNITED STATES and CANADA
Manhattan Publishing Company
1 Croton Point Avenue, P.O. Box 650
CROTON, N.Y. 10520

STRASBOURG
Mésange S.A.
Groupe Berger-Levrault
23, place Broglie
F-67081 STRASBOURG Cedex