2/83

STEIN SCHJØLBERG

COMPUTERS AND PENAL LEGISLATION

A study of the legal politics of a new technology

COMPLEX

NORWEGIAN RESEARCH CENTRE FOR COMPUTERS AND LAW

UNIVERSITETSFORLAGET

IBM Bergen: Dreggsalmenning 10/12, tlf (05) 31 55 00.
IBM Hamar: Parkgt. 2, tlf (065) 27 745
IBM Kristiansand S: Rådhusgt. 3, tlf. (042) 29 160
IBM Sarpsborg: Kirkegt. 63, tlf (031) 57 036
IBM Stavanger: Auglandsdalen 81, tlf (04) 58 85 00
IBM Trondheim: [redacted]gt. 60, tlf (075) 30 644
IBM Tønsberg: Nedre [redacted]gt. 33, tlf (033) 12 013.
IBM Ålesund: Parkgt. [redacted], tlf [redacted] 24 387
IBM Oslo: Dronning [redacted]gt. 10/11, tlf (02) 20 54 50

CompLex no. 2/83

Norwegian Research Center for Computers and Law
University of Oslo, Niels Juels gt. 16
OSLO 2

Stein Schjølberg

COMPUTERS AND PENAL LEGISLATION

A study of the legal politics of a new technology

Universitetsforlaget
Oslo

ISBN 82-00-06570-7
2. opplag 1983

Cover design: Sture Johannesson & Sten Kallin

The publication of the CompLex reports are supported by:
Bergens Tidende
Honeywell Bull
IBM
Norwegian Association for Computers and Law
Norwegian Association of Jurists
Norwegian Bankers' Association

Printed in Norway by GCS

To DONN -

father of the combat
against computer crime

P R E F A C E

As an attorney and prosecutor in the Oslo Police, I became aware of the computer technology and the impact on law enforcement and prosecutors in 1976 on a study trip to the United States. In the following years I felt the necessity of being informed of the experience with computer crime in countries where the computer technology was more adopted in the society, in order to be prepared for this development in Norway. Together with colleagues in Sweden and Denmark we invited Mr. Donn B. Parker to lecture at seminars in Scandinavia in 1977. With the assistance of the FBI I returned to the United States for more information on a study trip in 1978, and the Norwegian Ministry of Justice granted me leave of absence from August 1981 to July 1982 at SRI International in U.S.A. for further studies of computer crime.

Due to the introduction of computer technology in criminal activities it was obvious that at least two serious aspects of computer crime would challenge our traditional investigation and prosecution. It was necessary to develop the education and training of police investigators to keep pace with the development of this new technology, both nationally and internationally, and together with Interpol I was in charge of the first Interpol Training Seminar for Computer Crime Investigators in December 1981.

Another concern was the inadequacy of the existing penal legislation which was not written with computers and the automatic data processing in mind. Stretching statutes to other purposes than previously enacted is a problem prosecutors and courts dislike. Experience from the United States, West Germany, United Kingdom and Sweden revealed that some countries had considered this problem and enacted specialized

computer crime legislation. The internationalization of computer technology raises the question of harmonizing penal codes among the individual countries, and the OECD has initiated efforts of a questionnaire on the control of the computer crime, especially emphasizing the impact on the traditional, existing penal legislation. The evaluation of the answers from the member countries of OECD will take place in 1983.

This document, which contains the conclusions of the study and research at SRI International, is a presentation and evaluation of legal politics the computer technology causes in penal legislation.

The purpose of this document is to create an awareness of the problem in penal legislation in order to initiate similar evaluations in the individual countries, and not to present the conclusions. If this document together with the efforts of OECD result in the development of such measures in penal legislation with a view to the computer generation, the intention of the author is fulfilled.

Oslo, January 1983

Stein Schjølberg

Assistant Commissioner
Oslo politikammer
Oslo, Norway

ACKNOWLEDGEMENTS

This document has been possible after having spent approximately one year at SRI-International, Menlo Park, California, U.S.A. as an International Fellow. I am deeply grateful to SRI-International for having given me the invitation and the opportunity to study the problem of computers and penal legislation. Especially the guidance and cooperation with Senior Management Systems Consultant Donn B. Parker have been of great importance in my work. I would also be thankful to the other staff members within the Information Systems Management Center, among others Sandra Cook and Charles Wood, for their support and advice, and Louise Burnett for her secretary assistance.

The Norwegian Ministry of Justice granted me leave of absence from August 1981 to July 1982 to study this subject at SRI-International, and I am grateful for the Ministry's support.

The research project is organized as a program of the Norwegian Research Center for Computers and Law, Institute of Private Law, University of Oslo, described as TERESA (15). I am deeply grateful for the guidance and advice of dr. juris Jon Bing and the Institute's support in this research project.

I gratefully acknowledge funds from the International Communication Agency and the Board of Foreign Scholarships in Washington D.C. for a U.S. Government award under the provisions of Public Law 87-256, 87th Congress, the Fulbright-Hays Act, as a visiting Senior Fulbright-Hays Scholar. The award was made on the recommendation of the United States Educational Foundation in Norway.

I gratefully acknowledge funds from the Faculty of Law, University of Oslo; Johan Helmich Janson and Marcia Janson's Foundation, Norway; the Norwegian Bankers Association; the Norwegian Saving Banks Guaranty Fund; Honeywell-Bull, Norway; and Norwegian Data Centers Association.

Special thanks are given to Dagny Bjølsen, who has typed this document and prepared it for publication.

Stein Schjølberg

CONTENTS

SECTION I: INTRODUCTION

A. What is computer crime?

a. The development of computers in the society

Computers were introduced to our societies in the early 1950s. In the beginning the computers' complexity and cost limited their availability, but by and large they become less expensive together with a continuously improved reliability and capabilities. Especially in the 1970s a dramatic technological evolution occurred, creating the big computers and minicomputers of today[1].

The political, economic, educational and scientific institutions are increasingly dependent on computers in the industrialized countries, and other countries will experience the similar development, as they adopt the computer technology. Computers are being introduced to schools and homes, often described as personal computers, thus increasing the availability, knowledge and communications in the society. The predicted computerized society, the information age, is not far away.

1. According to ISO Vocabulary of Data Processing, developed by the International Standards Organisation, Technical Committee 97, Subcommittee I (ISO), a computer is defined as a functional unit that can perform substantial computation, including numerous arithmetic and/or logic operations, without intervention by a human operator during the run.

The development has created computer networks in the process of interchanging data between physically separated computers, increasingly both on national and international level, regarded as the most effective and economic method of communicating vast amounts of data. For instance, the banking establishments have in many years transferred funds between several banks through a computer network described as the Electronic Funds Transfer System (EFTS). And in recent years funds have been electronically transferred within the international banking community through a computer network[2] called SWIFT[3].

Computers are automatic devices that process data[4], most commonly today by electronic means[5]. Data represent information[6] of any kind, including computer programs[7] - the ordered set of data representing coded instructions or statements for the processing and storing of data.

2. A computer network is a complex consisting of two or more interconnected computing units (ISO).
3. SWIFT, the Society for Worldwide International Funds Transfer, introduced in 1978, and is regarded as the most secure commercial computer network in the world today.
4. Data is defined as a representation of information, knowledge, facts, concepts, or instructions, which are being prepared or have been prepared, in a formalized manner, and are intended for use in a computer system or computer network, as defined in the computer crime legislation in California, see note 7.
5. Electronic Data Processing (EDP) is data processing largely performed by electronic devices (ISO).
6. Information is defined as the meaning that a human assigns to data by means of the known conventions used in their representation (ISO).
7. Computer program is an ordered set of instructions or statements, and related data, when automatically executed in actual or modified form in a computer system, causes it to perform specified functions (as defined in Section 502 in the Penal Code of the State of California, enacted 1979).

b. Computers and criminal activity

As computers have developed, so have also crimes associated with their use. Mankind will always have to live with criminal activity, and as a result of the conversion to computer usage, new methods of perpetrating crime have occurred, using the new technology of computers. It is not surprisingly that people engaging in crime have discovered this new technique of storing or processing valuable data, representing money and property, or the value of the data itself. And with increasing usage, the potential of involving computers in crimes increases in proportion.

The description of this phenomenon has varied. Computer abuse, computer fraud, computer-related crime, computer-assisted crime, and computer crime are among terms used to identify this category of criminal activity, depending on the purposes of the descriptions. In the recent years, however, computer crime is regarded as the simplest, broadest and most widely accepted term in the criminal justice community and in public[8].

Computer crime has been presented and evaluated by several people, and has been a subject of research[9] as well as investigative[10] and legislative efforts in the recent years.

8. The U.S. Computer Crime Manual (see note 10) argues that "computer crime" implies direct involvement of computers in committing a crime, therefore the manual adopts the term "computer-related crime" to convey the broader meaning. But the manual accepts that "computer crime" is a common term used to identify illegal computer abuse, as well as using the term in the description of the manual itself.

9. The most exhaustive research has been conducted by Donn B. Parker, SRI-International (former Stanford Research Institute), Menlo Park, California, U.S.A.

10. The most important work is the Criminal Justice Resource Manual: Computer Crime, produced by SRI-International, for the Bureau of Justice Statistics, U.S. Dept. of Justice.

What is computer crime? As experience and technology have varied, so have also the definitions. The definitions have changed over the time with advances in knowledge and experience, and have revealed a necessity of a common definition in dealing with related aspects. What we understand with "computer crime" must be interpreted in the same manner, either we are evaluating the problem in penal legislation, investigation, security or research. The aspects and approaches are different, but they have at least one question in common, criminal activity and computers.

With the variety of aspects it is obvious that a broad definition is necessary. And for the purpose of the internationalization of data communication, a definition must also be understood and accepted throughout the world. On the other hand it must not be so broad, being useless in evaluating the different aspects, and must not only involve the present computer technology, but be a tool in the future generations of computers.

The definition must adequately separate this category of crime from other categories sufficiently. Since computer crime can involve crimes from murder to privacy violations, the definition must emphasize the particularity, the knowledge or the use of computer technology. Therefore, a widely accepted definition of computer crime encompasses <u>any illegal act for which knowledge of computer technology is essential for its perpetration</u> (investigation or prosecution)[11].

It is obvious that not every relation between computers and crime is a "computer crime". For instance, theft of computers and computer equipment is not computer crime if the perpetrator did not need more technological knowledge than stealing other

11. This definition was introduced by the manual prepared for the U.S. Dept. of Justice in 1979 (the full text)

physical property. Or in sabotage, destroying computers and computer equipment, without using any more knowledge than with destruction of other property. The perpetration or the intent in the act must involve knowledge of computer technology.

The decision must be made concretely, in a case-by-case evaluation. But the involvement of computer technology is fulfilled in all instances where the computer, the computer system or the computer network or data (also as programs) intended for use in a computer or in computer media (e.g. tapes, discs) are being used in the perpetration of an offence.

Computer crime can be divided in two main categories. In the first category, the computer can play a role as a tool of a crime, such as in fraud, embezzlement or theft of tangible property. In the second category, the computer is the object of the crime, for example in vandalism, appropriation or alteration of data, and obtaining computer services[12].

Criminal statistics throughout the world do not report any significant amount of computer crime. This may be due to the fact that most countries have not updated their Penal Codes to address such category of crime, and without this traditional means of identifying crimes it is not surprisingly that evidences of their existence are missing in such statistics.

12. Computer crime has been categorized in other dimensions. For instance, categorized by modi operandi: Physical attacks, false data entry, superzapping, impersonation, wire tapping, piggybacking, social engineering, scavening, trojan horse attacks, trap door use, asyncronous attacks, salami techniques, data leakage, logic bombs and simulation. U.S. Computer Manual, page 6.

Neither do traditional police statistics confirm any significant amount of computer crime. But a questionnaire through Interpol[13] has revealed that such crimes in fact are taking place. The police experience involves mostly computer crimes as fraud, theft of tangible property, embezzlement, which seldom creates a special challenge to the existing penal legislation, and will be handled routinely by police investigators and prosecutors. The answers from Interpol's member countries indicate, however, that investigation of new categories has occurred, for example erasure, alteration and appropriation of data, and illegal obtaining of computer services which involves more or less sophisticated use of computer technology.

Other efforts confirm that the existence of computer crime, for instance a survey through the Council of Europe[14], appeared from the late 1960s and increased in the 1970s.

In U.S.A. where the usage of computer techology expanded very rapidly in the 1960s and 1970s, many computer crimes have been prosecuted. But without the traditional means of identifying them it is difficult to estimate exactly. However, in a hearing before the U.S. Senate in 1978 the FBI, which investigates federal crimes, testified that they had conducted investigation in approximately 50 cases, mostly alteration of computer data input, but also theft of computer services, theft of data and alteration of data, as computer programs for either financial gain or destructive intent. It was emphasized, however, that most of the criminal cases were

13. See Appendix B.
14. Criminological Aspects of Econimic Crimes, 12th Conference of Directors of Criminological Research Institutes, Council of Europe, Strasbourg, 15-18 November 1976.
15. Joseph E. Henehan, Chief of the FBI's White-Collar Crime Section, Criminal Investigative Division, in a hearing before the Criminal Laws and Procedures Subcommittee, U.S. Senate, in June 1978.

prosecuted at the State level, and the FBI had no possibility of estimating the involvement of computer crime investigated by other police agencies.

Computer crime has been a subject of research, the most exhaustive conducted by Donn B. Parker, SRI-International, in USA. During the past 13 years, SRI-International has compiled a collection of over 1000 reported cases from around the world[16]. Parker states: "This collection does not necessarily represent the problem of computer crime, at the best it represents only a lower bound of incidences. The value of this research is describing offences involving computers in a case-by-case study, and in learning from actual experiences how to be more effective in dealing with a serious problem that has been proven to exist. The focus of this research is on examining the changing nature of crime as computers are increasingly used and relied upon, and not on collecting an exhaustive base of computer crime statistics."

There is a growing concern of a large amount of detected but unreported computer crime cases. This is not surprisingly from the experience in economic and other non-violent crimes. Victims, as governmental institutions, private organizations, and individuals are some times reluctant to report such crimes, fearing bad publicity, or loss of confidence, or more criminal attacks. In addition to this common attitudes, the computer technology, developed only in the recent three decades, is still exciting to the public, along with a tendency of not recognizing such crimes as ordinary crimes. In fact, the more sophisticated the computer crime, the more exciting the public finds it, and the victim is often more blamed than the perpetrator. Such attitudes can create serious effects on the victim while considering reporting the crime to the police,

16. A listing of publications, see Appendix C.

and to the police as well, because early reporting and cooperation from the victim is essential in police investigation.

Another reason of fearing many unreported computer crimes is that most countries have not yet updated their Penal Codes addressing the new methods of perpetrating offences in computer technology. Doubtful applications of the existing penal legislation have a tendency of resulting in other solutions than criminal complaints.

B. Computer technology and the vulnerability of the society

With the increasing usage of computer technology an awareness of a vulnerability in societies has occurred. Some countries have initiated efforts in evaluating such vulnerabilities, and have taken steps of preventive measures.

The increasing use of automatic data processing in individual countries represents at the same time an increasing national vulnerability. When governmental institutions and private organizations are relying upon the continuous availability and integrity of computer systems, operation of a relatively small number of technicians, processing and storing of valuable data, a new dimension of potential threat is at issue. Disturbance, errors or criminal activity may very quickly have a serious effect on operations of the society or organization, to an extent which was not possible in the manual systems. The concentration of data in automatic data processing, on individuals, transportations, communications, energy, financial information etc. has produced significant benefits, but it may also have a serious impact on the vulnerability of operations[17]. And with the potential threat from criminal activities, the extension of the problem of computer crime includes the national vulnerabilities of individual countries.

The transborder data flow will even more increase and expand this threat with the usage of international communications of data through telephone systems, satellites, radio systems, and optically, creating a new environment in criminal activity. Computer crimes are not limited to national borders, for

17. A study of the Vulnerability of the Computerized Society is presented by SARK, a Swedish Government Committee. This report discusses and evaluates various vulnerability factors, and a summary is available in English. It was published in 1979.

instance within a couple of seconds, a perpetrator in one country with the necessary knowledge and equipment is capable of erasing, altering or appropriating data in another country to almost the same extent this can be done within his own country.

An example of this transborder vulnerability is the one of the Fire Department in a Swedish town. The Fire Department uses a computer system for the turn-outs of fire alarm. In this system are stored important data on buildings, companies, water, electricity, and special fire sensitive places in the town. The system is run through a computer in the United States, and every fire alarm has a return ticket over the Atlantic Ocean.

One of the main efforts combating vulnerabilities in the society is adopting legislation in order to regulate, protect and prevent the automatic data processing violations. Such measures have been initiated in many countries, especially the aspect of privacy protection of personal data and individual liberties, described as Data Protection Acts[18]. Only a few countries have taken a step further in enacting additional penal legislation, encompassing criminal offences against all kinds of data[19].

On the international level, important efforts have been made by some organizations, adopting convention [20] and guidelines[21],

18. A status of Data Protection Legislation, January 1981, is presented by Peter Seipel, University of Stockholm, in Transnational Data Report, Vol. IV No. 1, 1981.
19. See Chapter III.
20. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, approved by the Committee of Ministers Meeting in Strasbourg, Council of Europe, September 18, 1980.
21. Organization for Economic Cooperation and Development (OECD) Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, adopted on its 523rd meeting, September 23, 1980.

introducing recommendations on protection of privacy and transborder data flow of personal data.

In order to successfully investigate computer crimes, police investigators and prosecutors must be offered special education and training. Governmental institutions and police organizations in some countries have already recognized such a need[22], as well as international police organizations[23]. The police organizations, which in the individual countries shall execute the society's obligation of investigating and prosecuting criminal offences, and participate in the preventive and deterrent efforts of penal legislation, must obtain the necessary investigative skill, maintaining control over and direct the investigation using the service and assistance of computer experts.

Experience from prosecutors has revealed that many computer crimes can be successfully prosecuted within the existing penal legislation, especially if the crime directly involves gain or sabotage of money and tangible property. In most countries the statutes of vandalism, theft, embezzlement and fraud apply as usual. The computer technology is merely used as a new tool or vehicle in committing these crimes. However, in the new categories of offences in computer environment the erasure, alteration or appropriation of data without such intent, the prosecution may face severe problems.

22. In the U.S. several organizations, including the FBI, have offered training courses especially directed on combating computer crime. In Canada, the Royal Canadian Mounted Police have organized similar courses.

23. The First Interpol Training Seminar for Investigators of Computer Crime was organized in Paris, December 7-11, 1981. Prosecutors and investigators from 25 countries participated.

An inadequacy of existing penal legislation could result in no charges against the perpetrator, or dismissal of the case or of some counts in the court. A disclosure or a potential of such vulnerabilities in penal legislation must result in enacting supplements in the statutes or specialized computer crime legislation. The preventive and deterrent effect of penal legislation must be maintained.

C. The outline of the discussions in this document

This document will discuss the automatic data processing and the impact on penal solutions. The old penal legislation was not written with computers in mind, and the question is whether the introduction of the new technology can influence penal solutions. If so, to what extent? The problem will be presented in Chapter III together with a discussion of various possible alternative solutions to the problem.

Statutes in penal legislation describe qualified unethical behaviour, in which the legislatures have decided punishment as a means to prevent and solve such behaviour in addition to traditional civil remedies. The evaluation of qualified unethical behaviour has developed over the years in the society, as offences against human beings and property have developed. In various aspects, codes of ethics and public sentiment of justice have been main resources for the legislatures together with court decisions. These resources have had the time to develop together with the human, financial and technological development in the society.

The development of automatic data processing has been so rapid and the impact on society so fast and enormous, with increasing applicability, that codes of ethics and public sentiment of justice have not kept pace. Therefore it is necessary to present and evaluate various behaviour in the automatic data processing (Chapter IV).

Such qualified unethical behaviour and the impact on existing penal legislation will be discussed in Chapter V. Is new penal legislation needed? If so, a model will be evaluated in Chapter VI. The conclusions for Norway will be presented in Chapter VII.

SECTION II: CATEGORIES OF COMPUTER CRIME

In order to discuss the impact on penal legislation it is necessary to present the most common categories of computer crime. The goal cannot be achieved without a basic understanding to what extent computers are involved in crime.

A. Theft, embezzlement and fraud of tangible property

As expected after the introduction of computers, perpetrators understood this new technology could be used as a tool in a crime, and after some time sophisticated methods developed, especially when programmers and computer operators were involved alone or in conspiracy with other perpetrators who could convert to economic gain.

The most common modus operandi in theft, embezzlement and fraud is data diddling[24] or false data entry. It involves changing of data before or during their input into computers. The changing can be made by anyone associated with or having access to the process of creating, recording, transporting, encoding, examining, checking, converting or transforming data that ultimately enter a computer. Examples are forging or counterfeiting documents, exchanging valid computer tapes, cards, or discs with prepared replacements, and source data entry violations.

Theft can involve all kinds of tangible property, including magnetic tapes and discs. The latter ones can be tempting targets when they contain data representing personal or financial information, or trade secrets.

24. U.S. Computer Crime Manual, page 9.

Some perpetrators have managed to alter or erase data, representing tangible property to show that it has been destroyed, damaged, or is obsolete, when in fact it has been stolen.

A typical example is the case of a computer operator in a company in U.S.A. who was able to steal products worth a considerable amount from his employer over a four-years period. To conceal the loss, he billed internal accounts in the computer system which were normally used to cover inventory disembursments that did not result in billings to customers, such as samples and exchanges. He used a debit invoice to cover the removal of products from stock, and offset it with a credit to the same account, so that it would not appear in the monthly statements. In his position, the computer operator was able to direct the printings of the computer so the company would have no record of the theft.

When property is appropriated and the perpetrator has aquired it by virtue of holding some office or position of trust, the perpetration is described as embezzlement. Especially when money is the subject, employees have discovered additional modi operandi of using the computer as a tool in the appropriation from their employer or its customers. One of the more sophisticated methods is described as the salami technique[25], whereby small amounts of assets are taken from a large number of sources, the principle being to take small slices without noticeable reduction of any source. For instance, in a banking system, the demand deposit accounting system for checking accounts could be changed to randomly reduce thousands of accounts by some cents, by transferring the money to a favoured account, from which the perpetrator can withdraw it

25. U.S. Computer Crime Manual, page 13.

through normal methods. The success of the appropriation is based on the idea that each checking account customer loses so little that it is seldom observed.

One of the most common computer crimes is fraud. The development of fictious personal data, contracts, accounts and companies is often more successfully accomplished in a computer system than in a manual system. Non-existent individuals' and companies' addresses are easier to "hide" in a computer system because continuous evaluation by human beings is lacking after the data have entered the system, and because the control actions fixed into computer programs are often insufficient.

Employee payment systems are particularly vulnerable to fraud. Fictious employees can be created, information on time cards or monthly or annual salaries for other employees can be manipulated. The individual employee will often not have the ability to check the calculations in his or her payment. This includes also welfare and pension payments. Fictious welfare claims have been presented in a large number of cases in U.S.A., and this seems to be a problem that will increase in the future as computer systems are being adopted in governmental institutions, especially when their employees are participating in the crime.

In one case, an employee at a Social Security Administration office in the U.S. used the computer to issue unauthorized benefit checks, totalling at least $ 100,000 to several accomplices outside the Social Security Administration. The employee was responsible for preparing documents for computer input and used that position to create the fraudulent benefits. Payment checks were automatically printed out after processing in the computer. The employee and the accomplices cashed the checks at various banks around the country. After checks were issued, the perpetrators managed to erase records of the transactions in the computer before the audit reports were produced.

When the management and the auditors are involved in computer crime, theft, embezzlement and fraud can be enormous. For instance, the Equity Funding Corporation case in U.S.A. in the early 1970s, where the management and officials of that company were involved in a mass conspiracy to defraud reinsurers, stockholders and customers. More than 60,000 fictious insurance policies were created and involved the manipulation of $ 143 millions. The false policies processed through the computer system were sold for cash to other insurance companies in the business of reinsurance. The fraud resulted in losses of over 2 billions dollars, including money lost by stockholders.

B. Sabotage and vandalism

Computers, computer facilities and data can be physically destroyed or damaged by arson, explosives, or other means. For instance, people have thrown car keys and screwdrivers into computers to destroy them. In the late 1960s and early 1970s several cases occurred in U.S.A. where computer centers were attacked, mostly by students, to express their political annoyance. In the last five years certain countries in Europe have experienced similar or more severe attacks. At least 30 such attacks have taken place in Italy and France, and one of the groups claiming responsibility for some attacks indicated that these attacks were the start of a systematic campaign against computer centers and companies in France. These serious crimes may create great damage to government, companies and society.

C. Automatic destruction of data

Data stored or processed on tapes and discs in a computer can be erased, altered or otherwise affected. This can be done physically by means of a magnet, or electronically by means of electro-magnetic pulses. In such instances the damage done to the data is not visible to human beings other than unappearance of human readable printouts or terminal screens.

The modi operandi of electronic destruction can vary from the simpler destruction, when the perpetrator intentionally erases data in communicating with data storage or processing units, to more sophisticated methods.

A logic bomb[26] is a computer program executed at appropriate or periodic times in a computer system that determines conditions or states of the computer that facilitate the perpetration of an unauthorized, malicious act. This logic bomb can for instance be inserted in the computer system with the use of the Trojan horse[27] method, which is the covert placement of instructions in a program so that the computer will perform unauthorized functions as well as allowing its intended functions. Programs are usually constructed sufficiently loosely, enough to allow space to be found or created for inserting the instructions.

In one case from the early 1970s in France, a young programmer dismissed from his job, devised such a scheme to express his annoyance with his employer. The programmer worked with a

26. U.S. Computer Crime Manual, page 21.
27. U.S. Computer Crime Manual, page 11.

program that would keep his employers' records[28] systematically updated on an annual basis. During his last weeks with the company he added to the program an instruction to destroy all records two years later. On New Years Day two years later, when the computer should have printed automatically the updating of all records, the printouts showed nothing. All data stored or processed in the computer for that purpose had been erased.

Based on the development in U.S.A. in the past three years, it is necessary to give a warning of what we may expect of electronic destruction in the future. A new computer generation of students is educated in computer technology. Several cases from U.S.A. and some in Europe indicate that this education also creates a potential for sophisticated computer criminals. Some of these students are challenged by beating the security in computer systems and accessing data files[29] and programs in governmental institutions and private companies as well as their educational institutions. With often unlimited amount of time at their disposal, they are sitting at their remote terminals attached to a telephone, trying to get into computer systems with dial-up access[30]. They have found a telephone number where the response is the high-pitched tone[31] of an on-line computer[32]. Once connected with a computer, it is only a question of seconds, minutes or days before such additional information as identification numbers

28. Record is a collection of related data or words, treated as a unit, e.g. in stock control each invoice could constitute one record (ISO).
29. File is a set of related records treated as a unit, e.g. in stock control, a file could consist of a set of invoices (ISO).
30. In data communication this action is taken to attempt to establish a connection between a terminal and another communication device over a switched line (IBM).
31. High frequency level.
32. Pertaining to the operation of a functional unit that is under the continual control of a computer. The term is also used to describe a user's access to a computer via a terminal (ISO).

and secret passwords are obtained. Further, experience shows that when such information is collected by one person, it has a tendency to be spread among other interested people, either through personal contacts or computerized bulletin board systems. These perpetrators are described as system hackers[33]. One of them has said that cracking a computer was like cracking a safe - only easier.

The system hackers are not necessarily destructive people, the challenge can be limited to accessing the company's data files or obtaining copies of data and programsas evidence of their successful act. However, some have gone further and erased or altered data and programs and even taken control over the computer. In one case the victim's computer print-out stated: "Welcome to my newly conquered HP 2000 time-sharing system". In another case: "I have now taken control over your computer"! Such perpetrators have managed to crash systems, erase or alter large quantities of data and programs, and denied others authorized use of the computer. Damage may amount into tens and hundreds of thousands of dollars in restoring and replacing data and programs, and even more in companies without backup copies.

In one case in U.S.A. the perpetrators were able to access a computer and destroy data and programs in another country through the telephone dial-up system. Four 13-year old students of the Dalton School in New York had received extensive instructions in computer technology. They used their experience in at least 41 telephone calls in 1980 to access or attempt to access 20 user files in a large Canadian time-sharing company and others involving Bell Canada, Honeywell, Pepsi-Cola, and universities in Canada. After several trial and error attacks,

33. Donn B. Parker, Computer Crime, page 107.

they were able to gain access to victims' files or parts of files. Backup copies were available so disruption and loss of time were small, but in one victim's files they erased one fifth of the data. It was assumed they obtained the correct telephone number from another source. The police got involved, and the telephone calls were traced to the Dalton School where the students were caught through a sophisticated investigation scheme[34].

34. The case was not prosecuted because of juvenile perpetrators.

D. Appropriation of data

Data processed or stored in computer systems can be appropriated without the taking of a physical object. In communication with a computer, perpetrators can obtain unauthorized access to data, and send the data to their remote terminals and appropriate the intellectual contents by reading or writing down the information, or by having the information printed at their terminal. The transfer of electro-magnetic pulses makes the property "taken" intangible.

When data represents financial or personal information, or trade secrets, it may be tempting targets to perpetrators. Great harm or loss to owners or legal users and to individuals results if such information becomes known to competitors or unauthorized people without the owner's consent and control.

One method of achieving such data is by impersonation[35], whereby the perpetrator accesses the computer by assuming the identity of an authorized user. He illegally obtains and presents to the computer the user's positive identifications, passwords, magnetic stripe card, or metal key. Electronic piggybacking[36] is another method. A hidden terminal is connected to the same line as an authorized user's terminal through the telephone switching equipment. The hidden terminal is used when the authorized terminal is not in use. The computer cannot differentiate between the two terminals, it senses only one terminal and one authorized user. The potential for wiretapping[37] increases as more computers are connected to communication facilities and larger amounts of electronically

35. U.S. Computer Crime Manual, page 25
36. U.S. Computer Crime Manual, page 25
37. U.S. Computer Crime Manual, page 27

stored assets are transmitted from computer to computer over communication circuits. But so far, known perpetrations of such cases have been rare, it is obvious that data can be appropriated more easily through other methods.

I have described the activities of the system hackers. In addition to having destructively erased or altered data, they have been able to appropriate data on identification numbers, passwords, financial statements, account balances, personal information and computer programs.

An example of appropriation of computer programs is the case of a former employee of a computer service company in U.S.A. who had supervisory authority for technical conversion and operation of a data center under contract to several federal agencies in U.S.A. Via telephone connection from his own terminal in another state the former employee was able to obtain account numbers and other information which were necessary for him to access the computer systems, exclusively used for the governmental agencies. Having access to this system, he obtained data representing a significant portion of a system's program. It was the system's program itself that was valuable, not the information of the federal agency. The perpetration was discovered by an employee in the company, who noticed that the computer was in use on an identification number belonging to a colleague who was present and did not use a terminal[38].

38. U.S. v. Seidlitz, 1978.

E. Theft of computer services

Theft of computer services or theft of computer time can vary from the employee who uses the computer to print Snoopy calendars or Christmas cards, or uses the services in processing private household accounts, to employees or other users taking advantage of the service far beyond their authorization or contracts. The latter instances can create great losses in terms of service value or cause great inconvenience. In some cases throughout the years perpetrators have used considerable portions of computer capacity and have made use of hundred thousands dollars worth of computer time.

Among the most serious cases is one from U.S.A. Two directors of an institute of technology were able to set up a data storage company within the institute's computer, and they served three business concerns, a medical magazine subscription company, an aircraft parts company, and an import-export company. They illegally used more than $200,000 worth of time on the computer, and the three private companies paid at least $40,000 in fees to the directors. Telephone lines were installed and tied into the institute's computer for use by the data storage company's clients. The usual access procedure was changed slightly, so that the institute's name was not mentioned, allowing the clients access. The crime was discovered when officials at the institute noticed that an increased amount of disc storage was being used, and the institute's computer was noticeably less productive.

Other employees have also utilized their employment. A computer programmer in a Board of Education in U.S.A. used his employer's computer system to set up a race-track betting system of his own and create computer programs for the benefit of a horse farm he owned. Such behaviour can reach almost

epidemic levels. In a case from U.S.A. an internal investigation in a governmental research center revealed that more than 200 employees had stored 456 unauthorized files for personal purposes in the time-sharing system used by the research center. Some of the employees were also connected to the computer system through dial-up telephone systems from terminals at their homes. The files included several hundred games, such as Star Trek and the like, poetry, jokes, personal letters, a beer can collection catalogue, etc. One of the employees had even used the computer system, assisting local gamblers run a bookmaking operation.

Legal users of computer systems have utilized their agreements with the owner of the computer system to purposes not mentioned in the contracts. In the following case from U.S.A. a company (A) was a legal user of a time-sharing system in a computer service company (B). The company (A) normally gained access to the computer system by dial-up, using a code which also was used by the computer company (B) to bill clients for time used on the system. However, the company (A) learned the codes of other customers (C) in the time-sharing system and used that information to alter the computer to charge other customers (C) for computer time it used for itself or for its clients (A). After the company (A) entered the computer system through its own account, the account number was changed to another customer's (C) account number, and when work was finished on the system, the company (A) switched back to its own account before signing off. It was discovered after some time, and the company (A) was fined and ordered to pay restitution.

F. Alteration and modification of data

In addition to altering data with destructive intent, data could be altered or modified with fraudulent intent and thus be used in illegal transactions. Or data representing legally relevant matter of fact can be altered and be used as evidence of a lawful right. This is the alteration of the computerized data itself, which can be compared with forgery of documents. As with forged documents the altered data can be used to defraud.

Some cases have revealed that students from their terminals have been able to alter grades for themselves and fellow students. These have varied from the more humorous to serious crimes. One group of classmates with computer education pulled a prank on their fellow students at a neighbouring rival school. The group of students were able to access the school district's computer system from their terminals, obtained the district's computer report card forms by some means, and printed out grades for all seniors at the rival school, giving them "F" in every subject. At the same time all seniors in their own class received straight "A" on their report cards. Parents of the latter students were reported to be overjoyed, and gave their children priviliges they would not normally get. The other parents were not happy at all, when they received the reports in the mail, until they were convinced it was a joke.

A more serious case occurred at a university in U.S.A. where the senior computer operator was indicted for falsifying 22 grades for one student and received approximately $300 for the job, and $100 from another student for falsifying 11 grades The tampering involved changing of data stored on computer discs in the university's grade records system.

Data can be modified with false intent by erasure or supplement of data in the computer system. For example, in U.S.A. a reckless driving offence of a chief of police was deleted from his record in the county's regional computer system through a terminal. The erasure was discovered during a routine inspection of a printout at the terminal where the charge was originally entered.

In another case from U.S.A. a records supervisor at a police department made a false entry into the national computer information system that a relative was wanted on charge of auto theft. The relative was detained on the charge in another state within a couple of days.

An employee of a computer company, working at a police department, was angry with his wife - so he put into the computer that his car had been stolen, knowing that she was driving it. The wife got picked up.

Obviously the most common purpose of altering or modifying data, as with documents, is the participation in other illegal or criminal offences. Fraudulent offences resulting in gain of money and property are for instance very often accomplished by the use of altered data. Such alterations are mostly simple changes of data, but may sometimes be very sophisticated. Interpol reports of a large bank which received a magnetic tape through the mail from an alleged major customer. The tape contained instructions from the customer to transfer 3 million dollars to various bank accounts. Due to a difference in the pulse rate of the tape leader and the identification code, controls in the bank were initiated, and an attempted major fraud was discovered. The tape had not been prepared by the customer, but by perpetrators who had opened the accounts with false identities.

In another case employees of a city and county data processing center in U.S.A. participated in erasing or altering data on their unpaid parking tickets, totalling at least 170 tickets over a period of 18 months. Data of the tickets in the computer system showed that they had been resolved or paid, but manual paper files reported the tickets still "open".

SECTION III: PRESENTING THE PROBLEM IN PENAL LEGISLATION

A. International efforts in computer crime legislation

a. Old Penal Codes and new technology

Traditional penal legislation protects physical objects, chattels, articles, paper and money against various categories of offences not accepted in the society. These objects are visible and tangible, and it is human understandable when protection against criminal activity is established. Economic value is not a necessity, also immaterial rights and values of affection are protected.

The development of penal legislation represents the development of ethical behaviour in most countries together with the development of technology in the society. The advances of technology in transportation, as airplanes and cars, and communication among human beings as telephone, radio and television, have resulted in regulation and protection against offences. Other technological advances, such as typewriters and copying machines, did not result in a need of special regulation or protection. The latter remedies have no potential themselves of harming human beings or society, and their use by human beings is regulated and protected through limiting the behaviour of the human being.

As with other technology, the development of computer technology must be evaluated in relation to penal legislation. The existing statutes in penal legislation were not written with computers in mind, and the main question is the applicability of these statutes on automatic data processing and to which

extent. The processing and storing of data by means of electronic impulses represent invisible and intangible values to governments, companies and individuals which clearly should be protected, and if the existing penal protection is not satisfactorily, solutions should be developed. And these questions must be solved in view of the international application of automatic data processing.

b. Computer crime legislation

Several countries have been aware of a legislative problem caused by the introduction of automatic data processing. Some have enacted or are proposing Data Protection Acts in order to regulate the collection, maintenance, use and dissemination of personal data[39]. The purpose of these Acts is to provide certain safeguards for the individual against an invasion of personal privacy. International organizations as OECD and the Council of Europe have made conventions and guidelines governing the protection of privacy and transborder flows of personal data[40]. For instance the OECD guidelines recommend "that member countries take into account in their domestic legislation the principles concerning the protection of privacy and individual liberties set forth in the Guidelines."

These Data Protection Acts do not give protection against ordinary criminal activities involving data, although they usually contain some limited penal statues emphasizing offences against requirements in regulations, unlawful disclosure of personal data, and the like.

39. See note 18.
40. See notes 20 and 21.

Some countries have gone further and enacted specific penal legislation, which includes offences against all kinds of data. These countries have chosen different approaches to a solution.

The Swedish Data Act, as other Data Protection Acts, protects personal data, but its Section 21 includes protection against ordinary criminal activity against all kinds of data. It reads as follows:

> "Any person who unlawfully procures access to a recording for automatic data processing or unlawfully alters or obliterates or enters such a recording in a file, shall be sentenced for data trespass to a fine or to imprisonment not exceeding two years, unless the offence is punishable under the Penal Code.
>
> Attempt at or premeditation of an offence referred to in the first paragraph shall be punishable under Chapter 23 of the Penal Code. If the offence, if perpetrated, were to be considered a minor offence, however, no penalty as said above shall be adjudged."

In West Germany three sections were enacted in the Penal Code in the late 1970s:

> "Section 263 A - Computer fraud:
>
> Anybody who, with a view to procuring himself or a third person any unlawful property advantage, causes prejudice to the property of another by influencing the result of a property-related data processing activity through the use of false data, or the distortion or suppression of true data, or by affecting the program flow, shall be sentenced to imprisonment not exceeding five years or to a fine, unless the offence is punishable under Sec. 263."
>
> "Section 269 - Alteration of stored data:
>
> Anybody who, with a view to defrauding in legal transactions, alters, without proper authority any data stored electronically, magnetically or otherwise invisibly, which, when processed in legal transactions, are destined to be used as evidence of legally relevant matters of fact, or uses any such data thus altered, shall be sentenced to imprisonment not exceeding five years or to a fine."

"Section 270:

Any fraudulent manipulation of a computer system constitutes fraud."

Until recently there was no special penal legislation in the United Kingdom on automatic data processing. However, with effect from October 27, 1981, the Counterfeit and Forgery Act became law. This Act has an interpretation of Part I, Section 8 (I)(d) in which forged "instrument" is defined as including "any disc, tape, sound track or other device on or in which information is recorded or stored by mechanical, electronic or other means." It is the purpose of this legislation that it could be used as a vehicle against the computer criminal who enters false information or alters any computer disc or tape with intent to defraud.

In U.S.A., 18 states (September 1982) have enacted computer crime legislation. A typical example of state computer crime laws is Section 502 of the Penal Code of California, which reads as follows:

"(a) .....

(b) Any person who intentionally accesses or causes to be accessed any computer system or computer network for the purpose of (1) devising or executing any scheme or artifice to defraud or extort or (2) obtaining money, property, or services with false or fraudulent intent, representations, or promises shall be guilty of a public offense.

(c) Any person who maliciously accesses, alters, deletes, damages, or destroys any computer system, computer network, computer program, or data shall be guilty of a public offense.

(d) Any person who violates the provisions of subdivision (a) or (b) is guilty of a felony and is punishable by a fine not exceeding five thousand dollars ($ 5,000), or by imprisonment in the state prison for 16 months, or two or three years, or by both such fine and imprisonment, or by a fine not exceeding two thousand five hundred dollars (2,500), or by imprisonment in the country jail not exceeding one year, or by both such fine and imprisonment.

(e) This section shall not be construed to preclude the applicability of any other provision of the criminal law of this state which applies or may apply to any transaction."

As with the other States this section of the California Penal Code has a definition of "property" as "including, but not limited to, financial instruments, data, computer programs, documents associated with computer systems and computer programs, or copies thereof, whether tangible or intangible, including both human and computer system readable data, and data while in transit."[41]

41. See note 4.

c. Preparation of computer crime legislation

Although Sweden has enacted the Section 21 in the Swedish Data Act, a committee is currently studying the relationship between automatic data processing and penal legislation, but has not presented any results yet[42].

Similar efforts have been initiated in West Germany where this question is the subject of a research project at the Max Planck Institute, University of Heidelberg.

In Canada computer crime legislation is being prepared by a special committee. A group of experts is studying the question, and is planning to include prohibition against theft of computer services, unauthorized alteration and erasure of data, and unlawful obtaining of data.

In Switzerland an expert committee responsible for revising a special section of the Penal Code is currently examining the question of computer crime.

Computers and penal legislation in Norway is a subject of a research project at the Norwegian Research Center for Computers and Law, The University of Oslo, and this document represents the proposal to the Ministry of Justice in Norway of enacting computer crime legislation.

In U.S.A. a federal Bill, "The Federal Computer Systems Protection Act", was introduced in U.S. Congress in 1977. It has been modified several times, but is still pending. The proposed 1981 version as an amendment of Chapter 47 of Title 18

42. The National Swedish Council for Crime Prevention has established a project on computer crime, which among other aspects of computer crime will study protective counter measures and transborder data flows' vulnerabilities.

in the United States Code reads as follows:

"H.R. 3970:

Section 1028. Computer Fraud and Abuse

(a) Whoever uses, or attempts to use, a computer with intent to execute a scheme or artifice to defraud, or to obtain property by false or fraudulent pretenses, representations, or promises, or to embezzle, steal, or knowingly convert to his use or the use of another, the property of another, shall, if the computer--

(1) is owned by, under contract to, or operated for, or on behalf of: (A) the United States Government; or (B) a financial institution; and the prohibited conduct directly involves or affects the computer operation for or on behalf of the United States Government or financial institution; or

(2) operates in, or uses a facility of, interstate commerce; be fined not more than two times the amount of the gain directly or indirectly derived from the offense or $50,000, whichever is higher, or imprisoned not more than five years, or both.

(b) Whoever intentionally and without authorization damages a computer described in subsection (a) shall be fined not more than $50,000 or imprisoned not more than five years or both."

In addition, the proposed federal Bill defines "property" as anything of value, and includes tangible and intangible personal property, information in the form of electronically processed, produced, or stored data, or any electronic data processing representation thereof, and services; and "services" are defined as "including computer data processing and storage functions".

d. Norway

The Norwegian Data Protection Act has similar purpose as other such legislation, to protect personal data against an invasion of personal privacy. Section 38 contains limited penal legislation of offences against requirements in the collection, or use, or disclosure of such data.

The traditional statutes in the Penal Code have not yet been updated to address computer crime, with exception of a supplement in Section 145 [43]:

> "Whoever, unauthorized breaks upon a letter or other closed document, or breaks into anothers locked depository, shall be punished by fines or by imprisonment for up to six months. The same applies to whoever unauthorized gains access to the contents of a closed communication or record when this ordinarily is accessible only with the aid of special equipment for hookups, replay, transillumination, reading, and the like.
>
> If injury is caused through unauthorized knowledge aquired thereby, or the felony is committed for the purpose of unlawful gain, imprisonment for up to two years may be imposed. Public prosecution may not be initiated without the request of the victim."

In reading this supplement it is difficult to understand it should have anything to do with computer crime, but statements in the preparatory process indicate that the supplement is not limited to telecommunication transmission as telegram and telex, but also data. And the term "recording" is used to include instances where the perpetrator gets knowledge of data stored in electronic media, using a computer or terminals.

Both the Norwegian Computer Association and the Penal Legislation Advisory Board in Norway, had critical remarks to the proposal. The Computer Association pointed out that including the new

43. An amendment of February 16, 1979.

technology in old Penal Codes should have been discussed on a broader basis, not modernizing certain statutes, and concluded with a statement that the supplement was not a step forward, recommending a broad revision of the Penal Code. The Penal Legislation Advisory Board pointed out that the Board found it doubtful in a statute protecting breach of letters etc., to include unauthorized access and knowledge of computer media, because of the differences in categories of instances they should protect, and the subject would possibly in addition involve other relations to data processing, which should be discussed. In spite of these advices the Bill was sent to the Stortinget (the Norwegian Parliament) and enacted.

Agreeing with all these remarks, and knowing the development in the computer technology and offences against computer media, it is obvious the supplement should not have been enacted. It should be enough to point out the quite different approaches in other countries.

On my own behalf I would in addition emphasize the complete lack of terms understandable to the society of producers, and vendors of computer equipment, and users of automatic data processing. One of the main tasks in penal legislation must be to prevent and deter offences which in turn may be a basis for good ethical behaviour in the environment protected. This is clearly not so in this instance, the supplement is almost not heard of, which is absolutely not the case of the Data Protection Act.

It is further obvious, knowing the seriousness in the offences involved in automatic data processing today, the maximum penalty is too weak. In addition both imprisonment and fines should have been made possible in sentencing together, as otherwise in similar modern penal legislation. And when the requirements of initiating public prosecution must be as with breach of

letters etc., knowing the variety of possible "victims" in data processing and the very difficult and serious problem of the ownership of data and programs, the conclusion is clear: The idea was good, but the result was more than worse. The supplement was evaluated too quickly, and when one asks for advice, one should also listen to advice.

The supplement must be repealed as quickly as possible in the broad evaluation of the old Penal Code which is now in progress, and replaced with computer crime legislation.

B. Approaches to solutions

a. The variety of solutions today

The presentation of the existing computer crime legislation in countries where such legislation is enacted or proposed, reveals a variety of solutions.

The proposed Federal Bill in U.S.A. and most of the computer crime legislation adopted in individual States within the U.S., represent the broadest solutions. This state legislation has, with some exceptions, more or less copied the proposed Federal Bill introduced in 1977 or later versions. The legislation includes fraud, theft, and embezzlement of tangible property and money gained by means of manipulating the computers as a tool in the offence. Such acts would also be covered by the traditional statutes of the offences mentioned, and for the purpose of penal legislation in relation to computer crime, such a solution should not be necessary in most countries. Traditional penal legislation emphasizes the gain of money and property, or categories of victims, but not the various measures to achieve this. Computers are merely used as a new way in old offences. These categories of computer crime legislation are obviously too broad.

The computer crime legislation in West Germany and Sweden seems to have in common attempts to fill the holes in existing penal legislation caused by the special nature of automatic data processing. The offences are typical categories of computer crime which would create unavoidable problems in traditional penal legislation. Although it is doubtful to include a statute involving criminal activities with all kinds of data in a Data Protection Act, which basic purpose is to protect

personal data. The known categories of computer crime go far beyond personal data, and from a preventive and deterrent point of view, such offences should be included in the Penal Codes.

The complexity in the German legislation would have a tendency to confuse the interpretation of the statutes. I would especially emphasize the term "affecting the program flow" (durch Einwirkung auf den Programmablauf beeinflusst), when "data processing" (Datenverarbeitungsvorgang) is used earlier in the same statute, and is the more accepted term. Section 269 uses the term "otherwise invisibly" (sonst nicht sichtbar gespeicherte Daten), while data can be processed or stored visibly by punched cards and optically with lasers.

The British Counterfeiting and Forgery Act of 1981 is the only step to a computer crime legislation with the definition including recording or storing of information. In other categories of computer crime as destruction and appropriation of data and programs, they have to rely on existing definitions in the Criminal Damage Act of 1971 and the Theft Act of 1968, of "property" and the like.

Another attempt to solve the problem with the extension of definitions is the one of the State of Virginia in U.S.A. In Section 18.2-98.1: Computer time, services, etc., subject of larceny, c 686 (1978) states that "computer time or services or data processing services or information or data stored in connection therewith is hereby defined to be property which may be the subject of larceny under Section 18.2-95 or 18.2-96, or embezzlement under Section 18.2-III, or false pretenses under Section 18.2-178."

Extension of definitions in penal legislation as the only means to address computer crime including the offences in the traditional statutes of theft, sabotage, fraud, and embezzlement etc.

challenges the basic rules of criminal juridical thinking. These statutes protect "property", "chattels", "items" and the like from criminal activity, and traditionally these are physically acts directed against tangible property. In theft, for instance the main principle is the intent of permanently depriving the owner of it, while appropriating data through remote terminals does not constitute a deprival of the data when the owner still has the data stored in the computer. When the appropriated data is computer programs and the perpetrator is printing them out at his own terminal using a printer, he is only copying the owner's program. The nature of such acts is totally different from the traditional deprival of property, and should be separated from the latter ones.

b. The significance of computer crime legislation

The description of the computer crime legislation and the efforts in proposing and evaluating such legislation in many countries indicate the recognition of a penal legislative problem in some categories of computer crime. If the question is whether computer crime legislation is needed or not, the answer would be clearly Yes, based upon our experience today with offences involving electronic data processing. The main reasons are at least two. The difficulties in the applicability of the existing penal legislation, see chapter V, and the deterrent and preventive purposes.

An essential task in penal legislation is to prevent crime. A potential perpetrator must be given a clear warning that specific offences are not tolerated by the society, and when this is not obeyed, he must be convicted for the crime explicitely done, satisfactorily efficient in order to deter him from further crime and deter others for doing the same. These basical principles must also be true in computer crime.

The development of automatic data processing is a new method of processing and storing data on property, money, facts, ideas, and other assets of great value to government, industry, and individuals. These assets must be protected in the same manner as physical objects. Data must be recognized as a protectable asset. The development of automatic data processing has often been compared with the development of automobiles, and as with the need of regulating and punishing non-acceptable driving, there is a similar need to regulate and punish non-acceptable acts involving data processing. And this legislation must be directed against these acts in a sufficiently related manner. In order to establish ethical behaviour in dealing with automatic data processing, specific statutes must be developed. To achieve this, it must be clarified in penal legislation what should be considered punishable, and one should not rely on difficult and less accessible interpretations of existing penal legislation.

This aspect is even more important as the development of computer applications and usage will increase rapidly in the future, along with the fact that a new generation of computer educated human beings will participate in this development. This human computer generation must in time also be educated in accepted behaviour in the automatic data processing. If no computer crime legislation is creating their behaviour, an uncertainty of potential threat and inconvenience to society will result.

With computer crime legislation perpetrators will be convicted for their explicit acts and not by existing statutes stretched in interpretation for the purpose, or by statutes covering only incidental or peripherical acts in the case. For example, two computer programmers in a large computer manufacturing company in U.S.A. developed over three years a computer program able to revise music into digitized form, selectively edit music, and print out any desired format, and they used their employer's computer in the development, totalling $144,000

worth of computer time. They set up their own company in order to sell the products, and used the mail in advertising and trading. Because of the latter acts they were convicted for mail fraud in addition to conspiracy, and not for unlawful use of the employer's computer.

When computer crime is recognized as a new criminal phenomenon in established computer crime legislation it will certainly ease the burden for prosecutors and courts. The evidentiary issues will be clarified and separated, and the courts will be able to participate in the process of establishing ethical behaviour more significantly through their ruling and sentencing. In court expert witnesses' testimonies will be able to explain technical aspects in the offence as in other criminal cases.

Computer crime legislation creates a need of educating and training of police investigators in the investigation of such offences. Through effective police agencies the potential threat to automatic data processing in the years to come, and the reluctance of victims to report such offences, will be reduced. Strengthening the law enforcement is one of the main efforts in preventing and deterring crimes, and in the field of computer technology, which is undergoing such rapid technological development, and which will have such a great impact on the operations of society, it is necessary to let this preventive measure be able to keep pace with the development.

The same reason applies to another aspect. Computer crime legislation will provide means of gathering crime statistics or police statistics, enabling governments to follow the offences on automatic data processing as they follow the development of other categories of crime. Without such legislation significant difficulties in evaluating the progress of computer technology will appear with the statistical structure in criminal offences today.

c. Harmonizing_Penal_Codes

The international nature of data communications through available telecommunications and computer networks, described as the transborder data flow, represents a specific aspect in evaluating computer crime legislation. In order to prevent offences across the borders and prosecute perpetrators, measures must be established.

With the variety in penal legislation and prosecutions in individual countries, it is obvious that the development of a transnational legislation would create more problems than it would solve. The approach must be based upon the national sovereignity and the individual Penal Codes.

But as the nature of data communications is international, so is also the nature of the offences on automatic data processing. Most categories of computer crime occur through similar methods of perpetration in all countries due to the environment of computer technology. If these categories are adopted in penal legislation in countries with transborder data flow facilities, the question of prosecution will be eased to the same extent as other internationally accepted categories of crime.

Through international organizations, efforts must be taken to ensure the similarity of offences on automatic data processing in the individual penal legislation. This can be achieved by means of conventions, or more likely as recommendations or guidelines. The individual countries will by such measures accept to enact specific computer crime legislation, or be recommended and encouraged to take such efforts.

Due to the difficulty on jurisdictional applicability when acts are committed in other countries than where the result occurred, and the high speed and flexibility of computers,

it should be evaluated in international measures, that each country adopts such penal legislation making it a crime to manipulate data or to use computers in other countries without legal access to such facilities in that country.

d. The relation to other solutions

When a victim has suffered from an act not authorized, disturbing or affecting his automatic data processing, other solutions than making it a crime or in addition to report it to the police are available, as with other non-violent crimes.

In the field of computer technology additional problems of uncertainty in the decision whether reporting the incident to the police or not appear compared to other categories of acts. Other categories of offences have developed over centuries or decades, and so have their ethical evaluations. Victims have experienced several acts which have resulted in more or less certainty in their judgements of the consequences and the impacts on the perpetrators. Automatic data processing has only developed the applicability over the past three decades, and the victims' experiences in judgements of unethical behaviour are minor compared to other categories of offences. This is first of all due to the rapid development in technology and various applications. The legislation, which in other categories has a great impact on the judgements, has not been able to follow up and cope with the development in order to govern and advise. For instance, Data Protection Acts are only very slowly adopted in countries with developed computer technology, and international guidelines and recommendations concerning protection of personal data were not approved or adopted until 1980. And criminal offences on automatic data processing have almost not at all been emphasized.

The lack of guidance from the penal legislation thus can explain the reluctance of victims to report the offences, and the tendency of relying on civil remedies as dismissal and damage when loss or inconvenience for themselves or the public occurs.

This has furthermore resulted in lack of codes of good practice in the automatic data processing. Slowly certain categories of unaccepted behaviour will be adopted in contracts, employees agreements etc., but the impact of penal legislation must participate in this process to the very best of all interests involved.

Also in the relation to other solutions than penal solutions, computer crime legislation is needed. Of course such legislation cannot go deeply in detailing the regulation and protection in governing the various behaviour in computer technology, but clarify certain unacceptable categories of behaviour as criminal offences in order to set standards.

With the vast amount of data and the great impact on operations of government, industry and individuals, it is obvious that the extent of this subject will include the future security of commerce, the national vulnerability of individual countries and the rights of individuals.

IV: A PRESENTATION OF VARIOUS TYPES OF BEHAVIOUR IN RESPECT TO COMPUTER SYSTEMS

A. Describing the purpose

In order to discuss the automatic data processing and the impact on existing penal legislation and the need for specialized computer crime legislation, it is necessary to present various types of behaviour and opinions in usage of computer technology as experienced today. When the question is whether certain types of behaviour should be qualified as criminal offences, evaluation of such attitudes is essential.

In Chapter II categories of computer crime were presented in relation to traditional juridical evaluation of criminal offences. This chapter will describe the concept of unethical behaviour in electronic data processing in some of these categories where the content of the behaviour is not clearly unethical and criminal today. Together it will hopefully point out the need for computer crime legislation.

Offences which are obviously unethical and made criminal offences in the existing penal legislation will not be discussed. Such offences include all categories of computer crime where the perpetrator is directly gaining money and tangible property as a result of the offence, by merely using the automatic data processing as a new remedy in committing the crime. In such offences the statutes of fraud, theft, embezzlement etc. are satisfactorily describing the unethical offence as a crime. The same applies to physical sabotage on computers, computer equipment and computer media - the statutes of sabotage clearly describe the unethical behaviour as a crime.

B. Studies on unethical behaviour

Two interesting studies on this subject have been presented in the recent years. Dr. John M. Carroll, Professor of Computer Science at the Univeristy of Western Ontario in Canada has presented a more informal survey on attitudes about ethics, and Donn B. Parker has in his book "Ethical Conflicts in Computer Science and Technology"[44] performed a very interesting study on this subject. Some of the scenarios and answers related to the purpose of this document will be quoted.

a. The Canadian study

Professor Carroll selected four groups of individuals in his study. The questionnaires were answered by senior computer science students at a university for two successive years, and by data processing professionals at a large bank (bankers) and a food distributing company (grocers). The answers were given anonymously and the results are as follows:

(the figures mentioned are per cent of yes answers)

	Students		Bankers	Grocers
	1977	1978	1979	1979
1. Do you believe it is ethical to offer the use of a program you have written at your employer's expense to a friend without your employer's permission?	29	28	0	0
2. Do you believe it is ethical to do work for one employer or client using computer time supplied by another?	48	76	36	7

44. AFIPS Press, Arlington, Virginia, USA. The study was supporte by a grant from the National Science Foundation in USA.

	Students		Bankers	Grocers
	1977	1978	1979	1979
3. Do you believe it is ethical to use a password to a time-sharing system that you discovered accidentally by making a mistake typing in your own password?	11	22	14	7
4. Do you believe it is ethical to attempt to do, for amusement, through a computer terminal things not described in the users manual?	59	51	36	21
5. Do you believe it is ethical to run personal programs after hours on your employer's computer?	36	38	21	14
6. Do you believe it is ethical to use a program known to you be proprietary in such a way as to avoid being charged for its use?	27	24	57	7
7. Do you believe it is ethical to rummage through trash baskets for interesting program listing?	27	16	14	0
8. Do you believe it is ethical to request a listing of a program from the computer, discover a comment statement saying it is the property of the time-sharing service, but use the program in another computer anyway?	25	33	64	7
9. Do you believe it is ethical to carry on business as a private consultant using computer time provided by your employer?	29	43	29	14
10. Do you believe it is ethical to copy your employer's system load modules onto magnetic tape you purchased and take them with you when you change jobs?	18	25	7	14

This survey reveals truly some interesting opinions. But as always in such answers to questionnaires, one must take into account the possibility of individual misunderstanding of the intentions of the questions. For instance, the similarity in questions no. 2 and 9 is obvious, although it is not reflected in the answers among the students.

Another objection is related to the questions, when the participants are asked whether it is ethical or not. The participants could have been more reluctant if they were questioned about their attitude to the similar questions using the term "unethical".

Not surprisingly the students have a high level of yes-answers in almost all questions. Their educational environment encourages more freely used data and computers, but it must be emphasized that one out of four students is willing to overlook written statements or other knowledge about the property of another as indicated in questions 8 and 10.

The survey reveals a significant difference in attitudes among data processing professionals in the bank and their colleagues in the food distributing company. The bankers seem to be less reluctant to use property and computer services belonging to another. One out of three bankers thinks that it is ethical to use computer time provided by their employer or supplied by another, note questions 2 and 9. Their attitudes on data as private property are surprisingly bad while working on the computer, note questions 6 and 9, but when the question is related to more physical removal in question 10 their answers indicate attitudes similar to what one should have expected if more theft-related terms had been used in the question. Additional evidence seems to be indicated in the answers in question 1.

The survey indicates, however, a tendency of opinions while working with data and computers. Surprisingly many do not find the same ethical problem in this environment as in that of only physical tangible property.

b. The SRI study

In 1977 SRI-International held a workshop on ethical issues in computer science and technology in Menlo Park, California. Prior to the workshop letters of invitation were sent out to selected people known of their interests in ethics in the computer field. These people represented a wide range of interests, including professionals with backgrounds in the computer field, ethical philosophers, psychologists, and lawyers from USA, Canada and the United Kingdom, who were all thought to be compatible in such a workshop. Along with the invitations 32 ethical scenarios were sent to the participants, inviting them to write their opinions about each actor and act and vote whether each scenario was unethical, not unethical, or not an ethics issue. These general votes were sent to SRI ahead of the workshop, and the results were compiled by Donn B. Parker, who conducted this project. At the workshop 35 people were able to participate in discussing and to vote in subgroups on 47 scenarios covering a variety of ethical aspects in the computer field. All voting was done secretly and anonymously. At the workshop some of the scenarios were discarded because of insufficient ethical issues, because the acts were clearly violations of law, or because the acts were clearly unethical, and several other scenarios were added. The participants discussed the scenarios in subgroups before voting on the actors and acts, as most of them had done previously by mail.

Some of the scenarios related to possible criminal offences will be presented in this document, but the study and the book written by Donn B. Parker are highly recommended for everybody concerned about ethical problems in various aspects of computer technology.

Scenario:[45a]

A university student used the campus computer time-sharing service as an authorized user. The service director announced that students would receive public recognition if they successfully compromised the computer system from their terminals. Students were urged to report the weaknesses they found. This created an atmosphere of casual game playing and one-upmanship in attacking the system.

The student found a means of compromising the system and reported it to the director. However, nothing was done to correct the vulnerability, and the student continued to use his advantage to obtain more computer time than he was otherwise allowed. He used this time to play games and continue his attacks to find more vulnerability.

Question: Student using computer service by taking advantage of a vulnerability.

Answers:

	Total	Unethical	Not unethical	No ethics issue
General vote	28	20	6	2
Subgroup vote	12	10	1	1

The majority of the participants stated the student's behaviour was unethical when he continued attacks for personal game playing.

45a: Donn B. Parker: "Ethical Conflicts in Computer Science and Technology", page 19.

Question: The service director encouraging compromise of the computer system.

Answers:	Total	Unethical	Not unethical	No ethics issue
General vote	17	9	3	5
Subgroup vote	10	2	3	5

Scenario: [45b]

The director of a federal government computer center noticed that significant amounts of computer time were being used by researchers in various research groups for game playing and other personal uses, such as generating "Snoopy calendars" (picture calendars produced by executing a computer program). These services were charged to the research projects.

He complained about this to the directors of the research groups, and they told him it was none of his business what their researchers did with their computer usage budgets. If they wanted to play games, that was all right, because it improved their computer skills and provided needed relaxing diversion.

Question: Research directors allowing researchers to make personal use of computer services.

Answers:					
	General vote	23	17	2	4

Question: Researchers making personal use of computer time.

Answers:					
	General vote	17	13	3	1

45b: Id. at page 22

Scenario:[45c]

A computer programmer in a large company had a personal interest in gambling games. He devised methods of calculating betting odds and studied new strategies. He noticed that the company computer was not normally used on Sundays, but power to the computer was kept on so that it remained in an idling state. Only a minor increment in resources usage would be employed in using the otherwise idling computer for useful work (the company charged users for all computer usage).

He decided that it might just as well be used when it was going to be idle. In fact, it would be useful to the company, because he could discover possible system failures and report them on Sundays to avoid costly delays on Mondays. He used large amounts of computer time for his personal activities on Sundays, using only negligible amounts of printer paper and producing only negligible additional wear. He did not request permission or report his usage, but he did not use deception either. The weekend guards logged his entries to the facility, and the use of the system was logged, but nobody checked the usage, and the leasing and maintenance contracts did not call for additional payments for the weekend time.

Question: Programmer using idle computer time.

Answers:	Total	Unethical	Not unethical	No ethics issue
General vote	27	22	3	2

In comments the participants stated that although negligible costs were involved, the programmer was unethical in using his employer's property without authorization. Though the programmer's act may not seem wrong in itself, what if all of the programmers did the same? If everyone exercised this alleged right, the results would be disastrous.

45c: Id. at page 25

Scenario: [45d]

A programmer employee of a time-sharing computer service company signed an agreement to purchase time-sharing services from a competing company. He used the services for over a year and promptly paid his bills. Nothing in the agreement he signed, messages to him from the system nor the users manual, issued him limited actions in the computer as long as he paid for the time used.

He routinely attempted to obtain copies of data and programs, i.e. other users' and the service company's files, to obtain copies of systems and utility programs[46], to identify other customers and ascertain their billings, to test programs without charge for which there is normally a charge, to gain privileged access available only to the service company employees, and he attempted to "crash" the system (cause loss of service to others).

He claimed there were no limitations placed on him to prohibit him from doing these things, and that he was simply engaged in accepted business intelligence activities and reverse engineering (General Motors buying a Ford to see how it is made and constructed).

Question: Programmer compromising and gathering intelligence on a competitor's time-sharing service.

Answers:	Total	Unethical	Not unethical	No ethics issue
General vote	28	26	2	0

Among other comments the participants stated that testing programs for which there is a charge without paying, the charge was nothing less than stealing. Gaining priviliged access available only to company employees was another form of stealing. Attempting to crash a system, unless authorized as a testing activity, is at least mischief, if not sabotage.

45d: Id. at page 41

46 : A utility program is kept in the computer and is available for all users. It provides such generally useful functions as sorting or trigonometry function calculation.

Scenario: [45e]

A commercial time-sharing service offered use of a program at a premium charge, the program to be used only in the service company's computer. A user obtained a copy of the program accidentally, when the service company inadvertently revealed it to him in discussions through the system (terminal to terminal) concerning a possible program bug. All copies of the program outside of the computer system were marked as trade secret, proprietary to the service, but the copy which the customer obtained from the computer was not. He used the copy of the program after he obtained it, without paying the usage fee to the service.

Question: Time-sharing user exploiting accidental access to a proprietary program.

Answers:	Total	Unethical	Not unethical	No ethics issue
General vote	26	24	1	1

45e: Id. at page 44

Scenario:[45f]

A manager in a computer facility quit his job and went into business as a consultant. He had been frustrated because he thought that his employer ignored his many suggestions for needed improvements, including better security to protect data and programs stored in a large, multi-access computer system. He had been given a secret password and was authorized to use it to gain access and use the computer services during his employment. At termination, the company did not tell him he was no longer authorized to the services, and did not invalidate the passwords.

The former manager returned to the company, offering his consulting services to assist in improving the computer security. The offer was refused. He then used the password from his own terminal and office telephone to extract copies of large amounts of data and programs for the only purpose of presenting the material to the company to show them the computer operation was insecure.

Question: Consultant using unauthorized access to demonstrate the insecurity of a potential client's computer operation.

Answers:	Total	Unethical	Not unethical	No ethics issue
General vote	28	18	9	1
Subgroup vote	11	10	1	0

Comments from the participants stated that it is understood that nonemployees should not have access to company records. Since he should not have had access, he was stealing materials. His motives, despite an altruistic element, did not excuse the act. His act was not only unethical, but illegal.

45f: Id. at page 55

Scenario: [45g]

A user of a commercial time-sharing service wrote and executed a program that called and used a utility program provided by the service. He obtained from the computer a copy of his program that included a copy of the utility program belonging to the service company. He used his program and the utility program on another time-sharing computer, run by a competing service company. The competing service wanted to use his program, and he sold them the program, including the utility program and all rights of use.

Question: User selling a package including a service company's utility program to a competitor.

Answers:	Total	Unethical	Not unethical	No ethics issue
General vote	28	25	3	0
Subgroup vote	9	8	1	0

All participants agreed that a user should not copy a program that belonged to someone else except for use as agreed. No one should sell the property of another. Almost all further agreed, that assuming the service company had properly protected its ownership through trade secret protection, this was a clear case of theft. Almost all disagreed with the statement that the time-sharing service company gave implied ownership to its users by allowing copies of their utility program to be made.

45g: Id. at page 64

c. Evaluation of the SRI study

Mr. Paul Strassmann, the principal author of the ICCP Code of Ethics, Conduct and Good Practice for Holders of the Certificate in Data Processing (Institute for Certification of Computer Professionals), did not attend the workshop, but has evaluated the major statements of the workshop participants. In a summary[47] he presents some Codes of Conduct from the scenarios, and the codes related to the purpose of this document are as follows:

Software or information developed during the course of business, using the employer's resources, is not the property of the employee. Having the power to subvert a system for an unauthorized purpose does not give one the right to do so, however scrupulous the effort to pay all costs and regardless of what subsequent actions are taken to remedy the subversion. Programmers do not have a property right in programs written or data aquired for others, even in the absence of any agreement stating this. A programmer or systems analyst should always seek direct and positive authorization for the use of data files or software programs from whomever he identifies, in his best effort, as the custodian/owner of the files or programs. Management of computer services must not encourage users to compromise a system.

Exploiting accidental access to proprietary software or data is unethical conduct. If such an event occurs, action shall be taken to notify the rightful owner and compensate for any gains realized.

Computer services, including supplies and data preparation, are a resource and should be conceived and used with care like any other economic resource. Computer time and facilities are

47: Donn B. Parker: Ethical Conflicts in Computer Science and Technology, page 153

an asset whose use should be justified by the purpose for which they are established, they are not for unauthorized personal use.

- - - - -

The statements in voting and discussions of these professionals in the study must be highly evaluated. Together with the summary of Mr. Strassmann they express at least two main principles.

Data, including computer programs as an ordered set of data, are assets like any tangible property or money. The concept of ethical behaviour in dealing with the latter objects applies also in dealing with data. It is clearly unethical to treat data otherwise than established in the rights of using them.

Computer services are resources like any other resources in governing the societies, production, financial operations etc. It is clearly unethical to use the computer services for other purposes than established without the consent of the rightful owner.

SECTION V: AUTOMATIC DATA PROCESSING AND THE INFLUENCE ON EXISTING PENAL LEGISLATION

A. New methods in old offences

Traditionally the intent of perpetrators committing crimes has been directed as violence of property and individuals, or gain of money and property, and the like. And the development of the existing penal legislation in various countries has mainly emphasized the protection of money and property with the assumption of tangibility.

In sabotage, arson and damage of property we are dealing with visible perpetrations. When the intent is gaining money and property we are assuming a visible removal of tangible property, or a visible fraudulent acquisition of tangible money and property. Although in some countries' penal legislation legal interpretations of property have been extended to comprise intangible property, these interpretations were not written with the computer technology in mind. The purpose of such definitions is mainly to include things like electricity, and more or less abstract interpretations of property, as a right or an interest in the property.

Automatic data processing can be used as a vehicle in these traditional criminal offences, resulting in visible damage of the tangible computer equipment, and visible removal or acquisitions of tangible money and property. When such perpetrations occur, the computer is merely a new method in the traditional offences, and the existing penal legislation will apply satisfactorily. In most countries the traditional statutes of sabotage, theft, embezzlement, fraud, extortion, conspiracy, malicious mischief and the like will be valid in these categories of computer crime.

B. The new assets

Data as the representation of facts, concepts or instructions in a formalized manner suitable for communication, interpretation or processing by automatic means are new assets. Physically the automatic data processing in computer systems or networks involves the processing of data from the moment they are entered at a terminal or other input devices, through the communication, and processing and storing of them, until the data appear in human readable language at a terminal or printer. This process is the vaults of the assets, wholly apart from the devices of communication or the data media themselves as magnetic tapes or discs, and this vault can be the "object" of criminal offences. But unlike the traditional offences against money and tangible property, the perpetrations are mainly invisible, only machine readable offences against clearly intangible assets.

These categories of computer crime cause concern and problems in the application of the existing penal legislation. The following discussions will evaluate the main principles in some existing statutes as they are recognized throughout most countries, and emphasize the vulnerable areas of applications and interpretations.

On the basis of these evalutations and this experience a model computer crime legislation will be presented in Chapter VI.

C. Sabotage, damage, vandalism, malicious mischief

When a perpetrator unlawfully and knowingly destroys, damages, renders useless, etc. the property of another, the offence is described with a variety of names in different countries. The main characteristic is the destruction wholly or partially of tangible property visible to human beings with direct or indirect display of power, or omissions.

Data, including also computer programs, are mainly invisible and clearly intangible, stored on tapes or discs, or processed electronically by handling of electric and magnetic pulses. An event of destruction is only machine readable and will not appear human understandable other than on a terminal screen or as a printout.

Is it justified to describe these data or pulses as "things" or "objects" within the traditional juridical thinking? And with the various methods in the destruction of data, will they satisfy the traditional terms in the existing statutes?

Some examples would clarify the problems:

A large commercial company in U.S.A. with worldwide access to its computer system through the international telecommunications network discovered in 1980 that they had some serious problems in their systems. Somebody was erasing files, creating files, modifying files by inserting pornographic words, and bringing the system down. The company soon found out that the attacks were from outside remote terminals. To publish the fact that the system had been compromised, the attackers also broadcast several obscene messages to system users. One group of users received the following message from the attackers:

> "The phantom, the system cracker strikes again, soon I will zero your disks and your backups on system A. I have already crashed your system B. Have fun trying to restore it you ...."

The company by telephone instructed users to change their passwords, but it was useless because the attackers had been able to establish privileged accounts of their own in the system. To keep the attackers off the system, the company had to shut the system down, examine all disc files for anomalies, recreate the disc system and regenerate the operating system. This remedial activity caused the system to be unavailable for almost two days. The company estimated the total cost associated with the series of incidents, which went on for three days, to a loss totalling $150,000. After satisfactory security measures were established and the case reported to the police, the perpetrators were caught. It was then discovered that they had used a home computer (micro-computer) programmed to emulate a computer terminal in accessing the company's computer system. The telephone number needed was obtained by automatic scanning using the micro-computer. The perpetrators were convicted under a State computer crime law. But the company was still receiving, until a year later, attempted attacks by other attackers on the average of once per week. It is suspected that the information about how to compromise their system was circulated through electronic bulletin boards all over U.S.A.

A 15 year old high school student in U.S.A. accessed the computer system used by the district board of education and wiped out data and programs over a period of three weeks, also including insertion of some obscene words in the system. He was caught and reported to the police. The data and programs used by the board were badly fouled up.

As earlier described, employees in commercial companies have expressed their annoyance with the employer in damaging data. Such damage may result in serious effects in operations of the companies. A dismissed programmer in a U.S. company programmed the system to erase a section of the memory bank whenever there was an input after he left the company, including the back-up unit. Two weeks after he left, the company discovered there were no data available in the computer system. The case was reported to the police.

Also governmental institutions have had disgruntled employees who wanted to harm their employer by some reason. Two employees in a State governmental institution in U.S.A. deleted arrest records of about 75 persons from their terminals over a period of almost a month. They were charged and pleaded to contest to a violation of the California Penal Code Section 594 (b) in 1978[48]. It may be noted that in spite of such an application of the existing statute of malicious mischief, the enacted computer crime legislation in California 1979 described in Chapter III, includes "Any person who maliciously accesses, alters, deletes, damages, or destroys any ... computer program or data ..."

Other data have been attacked. Interpol reports a case where a disgruntled employee of a printing company using a computer word processor, erased part contents of a book awaiting printing, and thereby causing damage valued at $ 3,000.

Most penal legislation is describing the destruction of property, or an object, or a chattel, or an article, etc. These descriptions mainly assume the physical tangibility, although some of them contain enacted interpretations,

48. This section is as follows: "Every person who maliciously injures or destroys any real or personal property not his own, in case otherwise than specified in this code, is guilty of vandalism. If the amount of injury or destruction is $ 1,000 or more, vandalism is punishable by imprisonment ..."

especially of "property" to include movable property or anything of value.

The application of the traditional interpretations of these descriptions in penal statutes on the communication, processing or storing of data in a computer is doubtful. When data communication is intercepted, resulting in erasure or modification of data, or stored or processed data are erased or modified, no tangible object is damaged. The data themselves are damaged, but they are not tangible.

Only when data are processed or stored on data media, as tapes or discs, the assumption of tangibility occurs, namely the media themselves. But when data are erased or modified, no visible damage appears on such objects, they represent no physical evidence of the destruction. At the best, the data media including their data, are rendered useless compared with the previous appearance. But again, as the medium itself is not rendered useless, the tape and disc are still capable of receiving and participate in the processing of data.

In any circumstances the differences in the physical concepts may create severe problems in the traditional juridical thinking of the applicability of the statutes of vandalism, sabotage, etc on automatic destruction. And even greater problems on the lay person, on whom the juridical system is wholly dependent in some court decisions. Stretching interpretations to other than previous purposes has a potential to confuse a jury.

Although no experience has revealed acquittals in courts, I will advise establishment of special computer crime legislation, encompassing the destruction of data.

It must be admitted, with expanded interpretations it may be possible to prosecute successfully such cases before a court. But a degree of uncertainty will always be present, especially where constitutional requirements are limiting such interpretations. And with a choice between such uncertainty and an undisputed statute, the decision should be easy.

In addition to this evaluation I will also emphasize the preventive and deterrent role penal legislation should play in the development of computer usage, and as a basis for ethical behaviour of the new human computer generation.

Almost all the enacted computer crime legislation on the state level in the U.S.A. as well as the proposed Federal Bill, are adopting legislation against destruction of data. In Europe, the Swedish Data Act, to the best of my knowledge, is the only legislation with similar statute.

As a conclusion no experience has revealed acquittance in prosecuted cases. With expanded interpretations it may be possible successfully to prosecute such categories of computer crime within the existing penal legislation, if such expanded interpretations are allowed. The necessity of specialized computer crime legislation must be based on other reasons, for example those presented in Chapter III B. In legislation without the possibility of expanded interpretations, new legal interpretations must be established, or an independent statute in a computer crime legislation should be established.

D. Theft or larceny of property

When a person unlawfully or dishonestly appropriates property belonging to another with the intention of permanently depriving the other of it, the offence is described as theft or larceny. The basic characteristic is the wrongful taking and carrying away the property without the owner's consent and without any claim of right, and use the property as his own.

The object of theft is in the penal legislation described as things, chattels, goods, articles and the like, and all these descriptions emphasize the tangibility, although the legislation sometimes has expanded the legal interpretation to include things in action, appropriation of electrical power, or other intangible property, or anything of value. The difficulties in the application of these descriptions of automatic data processing are similar to the automatic destruction of data. But unlike the destructive acts against data, the principle of stealing emphasizes "the removal" of the data. The perpetrators are human beings, and their unlawful gain is the information, defined as the meaning that a human being assigns to data by means of the known conventions used in their representation. The data are transmitted from the computer system of the rightful owner to the perpetrator's terminal or computer, and appear as information to the perpetrator on a terminal screen or as a printout.

The first question is whether the descriptions of the objects of theft apply to data and information.

In a case from U.S.A. involving the broader description "property", a Court of Appeals accepted computer programs as property within the meaning of the Federal Penal Code

Section 1343, Wire Fraud[49]. The case involved the appropriation of data as computer programs, and he was convicted on two accounts of wire fraud and acquitted on one count of transportation of stolen property across state lines. The violation of the wire fraud statute is the misuse of interstate communication devices such as telephones, to execute a scheme or artifice to defraud another of money and property. The defendant appealed the conviction and argued that the computer program did not constitute "money and property" within the meaning of Section 1343, but the Court of Appeals affirmed the conviction and held that the computer program was "property".

In legislation where the subject of theft is described as property, or even better as including intangible or movable property, the possibilities of a successful application on data are probable. However, it must be admitted that this legislation was not written with computer technology in mind, and the common interpretations are less suitable on automatic communicated, processed or stored data.

In legislation with more narrow description as objects, things, chattels and the like, it seems doubtful to rely on expanded interpretations. These descriptions are very much tied to the assumption of tangibility, and without additional interpretations enacted in the penal legislation it is likely that prosecution will meet serious problems in the courts.

Traditional statutes of theft assume the taking of an object, appropriating it when using it as the perpetrator's own. The content of the conception of "taking" assumes the physical removal from the owner. When data is obtained in automatic data processing by a perpetrator from a remote terminal, the data files or computer programs are still in the posession

49. This case is described in Chapter II D, U.S. v. Seidlitz, 1978.

of the owner. The perpetrator merely copies the owner's data on the terminal screen or as a printout of his own. Without expanded interpretations severe problems will arise in the application of traditional statutes of theft, especially if the statute contains description of a physical handling of the object. In the referred case from the U.S.A. U.S. v. Seidlitz, the defendant was indicted for violation of the Federal Code, Section 2314, which makes it a felony to transport stolen goods, securities or property across state lines. This count was dismissed in court by the judge, who ruled that the electronic impulses transmitted by telephone to a remote terminal in the defendant's state did not violate Section 2314.

Better possibilities occur in theft statutes which describe the broader concept, for instance the term "appropriates". An example is the Theft Act of 1968 in the United Kingdom, which in s. 3 (I) defines "appropriates" as "any assumption by a person of the rights of an owner amounts to an appropriation, and this includes where he has come by the property (innocently or not) without stealing it, any later assumption of a right to it by keeping or dealing with it as an owner". Data files and computer programs are belonging to a party, and when the perpetrator unlawfully or dishonestly appropriates the data even from remote terminals, it will satisfy the requirements in such a legislation. On the other hand, this definition in the United Kingdom interpreted in connection with the common law stealing, which was the wrongful taking and carrying away of any personal chattels of value out of the possession of the true owner, may result in a doubtful conclusion as to the copying of data would apply on constructions too much expansive from the traditional interpretation.

Notwithstanding the conclusions whether data or information is property, or whether the transmission of electronic impulses satisfies the interpretations of "taking" or "appropriating", the crucial test of the existing traditional statutes of theft is the requirement of an intention to permanently deprive the owner of the data. When the perpetrator appropriates data files or computer programs, he merely copies the data on his own remote terminal or as a printout at his terminal. The data will still be in the possession of the owner and to his future disposal. The perpetrator will very seldom have any intention of depriving the owner of the data, his intention is mostly to appropriate knowledge of what information the owner has stored in his data files, or knowledge about his computer programs, for instance as a competitor. If the intention is depriving the owner of the data, the perpetrator must erase the data in the computer, which will constitute an additional vandalism. With this requirement in the traditional statutes of theft it is obvious that these statutes very seldom will apply on the appropriation of data.

With the often extreme and crucial value of computer programs and data files to companies, scientific institutions and governments, it is interesting to evaluate the court experiences in such criminal offences.

Interpol is reporting one case in which an employee of an international car hire company obtained a printout of the customer list stored in the computer and sold it to a competitor. As in the penal legislation of that country information cannot be stolen, he was charged with theft of the printout paper.

In another case from Interpol a computer technician working for an insurance company used his terminal screen to consult a file on car insurance which had nothing to do with his work. Caught in the act, he admitted that he intended to use the information for his own benefit, and it was also established that he had taken away a computer printout. He was prosecuted for theft by an employee, and found guilty only of fraudulently removing a "listing of undetermined value". He was sentenced to imprisonment for two months, suspended for three years.

In U.S.A. a former computer service bureau employee was convicted of theft, when copying his former employer's computer programs before he left the company. He established a company of his own, using the computer programs. Although no conclusive evidence was presented, proving that the defendant in fact had copied the programs, the jury reportedly made its decision largely on the basis of expert testimony that stated it would be impossible to recreate the programs so precisely in the short amount of time that had elapsed between the time the defendant left his former job and the time he started his own firm. It is not reported by what method he used to duplicate the programs, the possibility of using his former employer's tape or discs is one of the methods. He was fined $50,000, and an appeal is still pending.

Data can achieve specialized legal protection. Data bases and computer programs can be copyrighted and be a subject of trade secret. Violations of such specialized protection are in many countries under certain conditions criminal offences.

In relation to unlawful automatic appropriation of data bases and computer programs, the most practical protection is the trade secret protection. The basic principle of

copyright protection is that only the manner in which the ideas are expressed are subject to copyright protection, not the idea itself. Copyright protection protects only the copying of the product, not the use of it, and does not exclude other parties from adopting the ideas, or in other words, appropriate the ideas.

Data bases and computer programs may be subjects of trade secrets. The main characteristic of trade protection is the secrecy. The owner of data and computer programs must establish measures to limit the general public access to them, and if they are traded to other parties, the secrecy must be limited in contracts, licenced, or in employee, or customers, or consultant agreements, in order to restrict the distribution.

When satisfactory efforts are taken to keep data bases and computer programs secret within the meaning of the individual trade secret legislation, unlawful appropriation would be a criminal offence if penal statutes covering such appropriation exist, and if the owner satisfies the individual conditions of trade, and commerce, and the like.

The advantages in the application of trade secret penal legislation are that such legislation does not require an intention of permanently depriving the owner of the data, and that the requirements of "appropriation" have a tendency of a broader understanding, not limited to descriptions of physical taking and the like. In addition it is seldom a question of economic evaluations of the secrecy appropriated. On the other hand such offences have a tendency to be described as a misdemeanour, though it is of great value to the owner, especially computer programs. But the main objection is the limitation of the penal trade secret legislation itself, data bases and computer programs are not always trade secrets. Trade secret legislation cannot

substitute other penal legislation in unlawful appropriation of data and computer programs, only as before, additionally specialized penal legislation.

Theft related criminal offences, as embezzlement and receipt of stolen property,will meet similar difficulties in the application of automatic data processing. When the perpetrator has aquired data by virtue of holding a position of trust - for example by contract - is using a time-sharing system, and while using the data bases and programs at the same time is transmitting all the data to his own computer system, the problems of describing data as "property", "chattels" and "taking" are similar to theft. In addition, it is doubtful that the perpetrator in such instances is in a legal possession of the property, when the data still are in the owner's computer system, and can be used by other parties. Only the traditional physical possession of the discs and tapes seems to fulfil this requirement.

The assumption of permanently intention of depriving the owner of the property is also required in embezzlement and receipt of stolen property, and as evaluated in theft, it is probable that such a requirement is not fulfilled when the owner still has the possession of the data, or has his tapes and discs returned, and the perpetrator merely has copied the data. The only thing the owner is deprived of is his exclusivity.

As a conclusion it is highly unlikely the traditional statutes of theft, embezzlement and receipt of stolen property apply on the automatic appropriation of data. Without expanded interpretations, prosecutions could fail in courts, or at the very best challenge the luck in a manner not appropriate in common prosecutions.

Even with expanded, enacted interpretations in penal legislation the appropriation of data by automatic means is far

beyond the traditional taking or carrying away property. To establish purposes in penal legislation quite different from the previously enacted is doubtful from a constitutional point of view, and will distance itself from the interpretations of the lay person and thus challenge the very important preventive and deterrent role of penal legislation.

I clearly recommend the establishment of specialized statutes encompassing unlawful appropriation of data.

E. Forgery and counterfeiting

Making use of forged or counterfeited documents is in many countries a criminal offence, if the intent is to defraud another, or if the intent is to use them as evidence of a legally relevant matter of fact. Using such documents as genuine establishes forgery, even without handwriting or signature.

The concept of "document" varies dependent on the interpretations, and many countries include more than traditional writing, for example seals, emblems, sound tapes and gramophone records. In fact any object capable of expressing human intimation may be a "document" or an "instrument", which in some countries is the legal description of these "objects" today[50]. However, an essential distinction is the difference between false documents and documents containing incorrect statements of facts. False documents do not represent, or only partially, the meaning of the alleged issuer. Incorrect is the document if it contains facts not true, but genuine in execution.

The application of existing statutes of forgery on automatic data processing may offer serious problems. Forgery of supporting documents before entering the data into the computer may be handled traditionally as forgery or counterfeiting documents. But what about printouts from the system after the data are processed by the computer? This was the issue in the Appellate Court in U.S. v. Jones[51] (1977). The defendant was indicted for altering accounts payable data and feeding the data into a computer that issued checks payable to a fictious account, totalling five checks that resulted in $130,000 to the perpetrators. The sole issue was whether the

50. See "The Forgery and Counterfeiting Act of October 27, 1981 in United Kingdom.

51. American Criminal Law Review, Volume 18, number 2, Fall 1980 page 377, and SRI- Internationals User Manual for the SRI Computer Crime File on the Juris System, U.S. Department of Justice, page 39-41.

alteration of accounts payable documents fed into the computer, which resulted in the issue of checks payable to an improper payee constituted a "falsely made, forged, altered, counterfeited or spurious security within the meaning of the exclusionary clauses of sections 2314 and 2315 of Title 18 in U.S. Code."

The Appellate Court analysed the facts as follows:

> "In the present case, the district court was of the opinion that the defendant, in fact, made a false writing because "the individual who drafted the instrument in a practical sense was the defendant, although he employed the computer as the instrumentality by which the checks were physically drawn". We think, however, that the acts of the defendant did not constitute the making of a false writing, but rather amounted to the creation of a writing, which was genuine in execution but false as to the statements of fact contained in such writing. The distinction is critical to the sufficiency of the indictment.
>
> The district court was of the opinion that the facts did not warrant the conclusion that false statements appeared on the face of the checks issued by the victim company to the fictious account. We cannot agree. The checks state that the designated amount is payable "to the order of the fictious person", and implicit in such an unconditional order was the existence of an obligation running from the victim to the payee. There was, of course, no such obligation, but as the result the victim was defrauded into believing that the company owed a bona fide obligation to the fictious person and, accordingly issued a genuine instrument containing false statement of fact as to the true creditor.
>
> Since we conclude that the checks did not fall within the exclusion of the statutes as forgeries, the order of the district court dismissing the indictment must be reversed."

With such an understanding of printed documents from the computer after being processed in the system, it will not constitute forgery as described in existing statutes. Instead one must emphasize to make use of forged or counterfeited

supporting documents before converting the data to automatic processed data.

When computer-prepared documents are facing problems on the application of existing traditional criminal statutes, it is not surprising that some countries, as described in Chapter III, have taken efforts to enact specialized computer crime legislation, including the even more difficult problem: The alteration or modification of data within the automatic data processing. Such offences can be done directly from terminals without the necessity of falsifying supporting documents before the data are entered in the computer. The "forged" results in appearance on terminal screens or attached printouts.

Even with a broad interpretation of "document" or "instrument" severe problems occur, including the data on tapes and discs. The tapes and discs themselves could be evaluated as documents, but the processing, storing and communication of data create a new and unique environment of presenting information to human beings. This process is not a physical object, which normally is the assumption of documents, nor has the automatic data processing any significant similarity with other assumptions. It is doubtful that all categories of automatic data processing express human intimation, and unlikely that the processing of data represents legal effect or the foundation of legal liability. Such results can only be achieved when the data is converted to information for human beings.

As a conclusion it is highly unlikely that the traditional statutes of forgery apply on the electronic alteration or modification of data. Expanded interpretations of "documents" or "instruments" encompassing data seem far beyond the traditional meaning of such terms.

It is necessary to introduce specialized penal legislation including this category of computer crime. In efforts to achieve such legislation two methods can be chosen, either enacting special legal interpretations as e.g. in the Forgery and Counterfeiting Act of 1981 in the United Kingdom, or independent computer crime legislation as the Section 263A and Section 269 in the Federal Penal Code in West Germany.

I clearly recommend enacting independent statutes. Not only because statutes covering other categories of computer crime are necessary, as described in this chapter, but also from the preventive and deterrent point of view. The preventive effect of penal legislation improves when the offences involved are clearly described in the statutes. And the environment of automatic data processing differs much from the traditional environment of falsification of documents.

F. Unlawful use of property

In many countries the unlawful use or unauthorized use of property or an object belonging to another is a criminal offence. The characteristic is the use of an object, dishonestly obtaining an advantage or service without any intention of depriving the owner of the object.

The unlawful use may be obtained by a perpetrator without any rights or authority to the object, but also by a party allowed using the computer as a legal user, when it is used beyond the agreements in contracts or by employment.

In automatic data processing the property or the object is the computer or the computer system, or discs and tapes containing data. As other property these objects can be used without authorization, and experience has revealed that unauthorized use of computers or computer systems has occurred to a great extent, as described in Chapter II.

Although the data itself is not an object within the traditional meaning of the term, the computers, discs and tapes are, and thus normally create no challenge to the application of such penal legislation.

Some statutes of unlawful use require an additional deception of another, thus covering instances where the perpetrator obtains the use or services with no intention to pay for it. Such more narrow statutes are not satisfactorily in the application of all categories of unauthorized use. They do not appear to catch the case of one who, while quite willing to pay for the services, upon being denied access legitimately, secures it illegitimately by some subterfuge.[52]

52. Colin Tapper: Computer Law, page 109

A very interesting case involving a special requirement in a "use of service" statute occurred in Canada. The Supreme Court of Canada made an important decision whether the Canadian Criminal Code applied on an unauthorized use of computers[53].

Three students at the University of Alberta were able to access the university's computer system from a terminal in another building at the campus through telephone wires. They were able to establish unauthorized accounts for themselves by altering the systems accounting records, and reserved portions of the memory for their own use. The unauthorized use, totalling a vast amount of time, went on over a period of several months. In addition the system was crashed several times. Their activity caused severe damage and inconvenience to legal users.

In the court one of the students was acquitted of all charges, one was convicted of mischief under Section 387(1)(c), and the third was convicted of theft under Section 287(1)(b) but acquitted of mischief. The third student appealed and was acquitted in The Court of Appeals, and this acquittal was affirmed in the Supreme Court.

The third student was charged and convicted under Section 287(1)(b) which reads as follows:

> "Everyone commits theft who fraudulently, maliciously, or without colour of right,
>
> (a) abstracts, consumes or uses electricity or gas, or causes it to be wasted or diverted, or
>
> (b) uses any telecommunication facility or obtains any telecommunication service."

53. The Queen v. McLaughlin. An evaluation of this decision is made by Robert P. Bigelow in Computer Security Journal, Spring 1981.

Subsection 2 defines "telecommunication" as "any transmission, emission or reception of signs, signals, writing, images, sounds or intelligence of any nature by radio, visual, electronic or other electromagnetic system".

The historical purpose of this Section was to encompass the use of a telephone or telegraph line or the obtaining of telephone or telegraph service maliciously or fraudulently.

In his vote the Chief Justice Laskin emphasized the following question:

> "I have no doubt that a computer system may be termed a "facility", as being something built, installed or established to serve a particular function or to accomplish some end or provide a certain service. Is it however, within the definition of "telecommunication" in Section 287 (2) ?
>
> "Transmission ... or reception of ... intelligence of any nature" connotes to me, in the light of the history of Section 287, that what is aimed at is the theft of information from a facility through which it is channelled. True, what is involved here is an electronic system, but the function of the computer is not the channelling of information to outside recipients so as to be susceptible in that respect to unauthorized use. Rather, it is to permit the making of complex calculations, to process and correlate information and to store it, and to enable it to be retrieved. The distinction I would draw is, admittedly, narrow. However, I do not think that using a terminal, as did the accused, to plug into the central processing unit and to retrieve information stored there brings such use within Section 287 (1)(b). The use of the terminal itself would not bring Section 287 (1)(b) into play, and the fact that the accused, by using the terminal, was able to make electronic connection with the central processing unit to capture information that was stored there does not advance the case against him.
>
> What is involved here is a data processing facility rather than a telecommunication facility, although it incorporates electronic equipment. Taking the facility as a whole (the central processing unit and the terminals) there was no transmission or reception externally. Although there was transmission of intelligence from one part of the facility to another, there was no

> reception by other facilities nor emissions from this facility. In my opinion, the conduct of the accused is not so clearly caught by the statute as to warrant a conviction thereunder."

This vote of Chief Justice Laskin is very important for several reasons. It is one of the very few opinions from the Supreme Courts around the world directly evaluating automatic data processing, data communications and criminal offences. The vote clearly emphasizes the difficulties in using statutes enacted for other purposes, on electronic offences, and the constitutional requirements in penal legislation. As stated by the secondary voting Judge Estey:

> "I adopt entirely the observations of the Chief Justice with reference to the proper interpretative technique to be used when construing a criminal statute. Had Parliament intended to associate penal consequences with the unauthorized operation of a computer, it no doubt would have done so in a section of the Criminal Code or other penal statute in which the term which is now so permanently embedded in our language is employed. The Court would not be expected by Parliament to glean from writings generally associated with the communications industry an intent to attach penal consequences to the unauthorized operation of a computer."

As a conclusion, in penal legislation without any additional requirements in the statute other than the unlawful use of anothers property or objects, the statute applies on unauthorized use of computers or computer systems. But one main objection in such legislation is that the offences are mainly misdemeanours, which with our experience so far seem too weak to be dealing with the great losses to the owner of the computers. Another objection is, although the statutes apply they are generally written, the preventive and deterrent role of penal legislation in the future society of widespread computer usage must result in specialized statutes directly emphasizing the unauthorized use of computers and computer systems and data communications as a criminal offence.

In legislation with additional requirements in "use of property-service" statutes, these requirements tend to make the applications a serious problem.

I clearly advise enacting penal statutes, making the unauthorized use of computers, computer systems and data communication facilities undisputed criminal offences.

SECTION VI: COMPUTER CRIME LEGISLATION - AN INTERNATIONAL MODEL

A. Legislative technique

a. Enacting interpretations or independent statutes

The use of enacting interpretations in penal legislation varies among the countries. Some countries are very reluctant to include interpretations, a tendency among continental European countries, and others are more willingly, as the Anglo-American penal legislation. Thus, the question of expanding the interpretations arises more easily in the latter area of penal legislation.

When new categories of offences occur, causing a need of supplementing the penal legislation, the continental European traditions tend to create new or altered statutes, including the new offences.

Solving this problem is a basic constitutional question in sovereign countries. The model penal legislation in this document is intended on emphasizing the new offences due to the introduction of automatic data processing, and the necessity of enacting supplementary penal legislation. It is only a guideline or recommendation, and the countries must adopt this proposal, if needed, within their individual traditions. The main idea is creating an awareness of the problems in order to prepare the countries on an increasing, international problem.

b. Computer-related terms in penal legislation

The computer technology has invented a new terminology, some terms only used within the computer society, and some more or less adopted in public language. When considering specialized terms in the penal legislation, only terms of the latter category must be evaluated.

It is obvious that the more technical terms as "bits", "bugs" and the like must be avoided. Some current computer crime statutes use the term "software" either in the statute itself[55] or in supplementary interpretations in the statute[56]. Also this term must be avoided, not adopted in public language and more or less artificial, thus confusing more than educating.

The term "computer program" is used in the penal legislation in some of the States in U.S.A. in addition to "data"[57]. As described in Chapter I, a computer program is an ordered set of instructions or statements and related data, or to put it short - an ordered set of data. The use of "computer program" should be avoided as unnecessary in addition to "data".

"Data" is adopted in public language and is a basic term in computer technology. This is the description of the "object", which the computer crime legislation protects, and thus it must be included in any such legislation. The experience in the various enacted computer crime legislation today confirms this. All of them, except one, namely the Forgery and Counterfeiting Act of 1981 in the United Kingdom, are including the term "data".

55. The State of Arizona C.204 §13-2316B (1978)
56. The State of Florida H.B. 1305 Section I (1978)
57. The State of Georgia H.B. 198 Section 4 (b) (1981)

Not surprisingly, knowing the experience from various enacted Data Protection Acts, the English exception uses the term "information". These Acts, in which some use "data" and some "information", indicate a confusing ambiguity regarding the concept of terminology. As described in Chapter I, "information" is the meaning that a human being assigns to data. The data will always be the genuine, the meaning we assign to them always a substitute.

Similar confusions have arisen in descriptions of devices in automatic data processing. Due to the rapid technological revolution or evolution, a device modern today may be old-fashioned in some years. The main approach in computer crime legislation is the protection against and the regulation of misuse. As Donn B. Parker has expressed to the U.S. Senate: "Do not try to exclude devices when the real purpose may be to exclude certain uses."

Therefore it is recommended to describe devices generally, not specific, and certainly not directly exclude devices in enacted legal interpretations[58].

58. For example, the proposed Federal Bill, H.R.3970 in U.S.A., defines "computer": Meaning a device that performs logical, arithmetic, and storage functions by electronic manipulation, and includes any property and communication facility directly related to or operating in conjunction with such a device, but does not include an automated typewriter or typesetter, or any computer designed and manufactured for, and which is used exclusively for routine personal, family, or household purposes including a portable hand-held electronic calculator.

c. Questions to be solved in individual countries

Statutes including accessory to or attempted criminal offences vary among the countries. The model will not discuss these categories, but recommends such aspects incorporated in computer crime legislation similar to those of other categories of crime against property.

Another question is the punishment. Similar to other serious crime against property it is clearly recommended evaluating computer crime legislation as a felony with similar maximum imprisonment. The often extreme value of data must result in protecting the owner with maximum efforts against offences in automatic data processing. One of these measures is the preventive and deterrent effect of penal legislation. On the other hand petty offences should as always in penal legislation be treated reasonably and/or as misdemeanours. But to do as in the Swedish Data Act, Section 21, which reads as follows, is probably giving too much away:

> "If the offence, if perpetrated were to be considered as minor offence, however, no penalty as said above shall be adjudged."

The difficulties in the separation of a "minor offence" in criminal offences against data may in such statutes reduce the very important preventive effect of penal legislation.

As in other modern penal legislation, both imprisonment and fines must be included in the statutes, enabling the courts to use both categories of punishment at the same time.

d. Description of devices

The rapid development of data processing technology creates problems in drafting the legislation. The constitutional requirements in penal legislation of satisfactorily individualizing the offences made criminal, create an even greater problem than in Data Protection Acts or other legislation. But to some extent, reasonable interpretations are accepted.

When data processing developed from manual handling to other measures, the evolution involved devices processing the data by mechanical, magnetic and electronic operations. Today processing of data by optical devices, as by laser, is developed, and in the future other means, as biological processing of data, is a scientific prediction. The term "electronic data processing" is most commonly used to encompass all practical data processing other than manual in the society of today, and is widely adopted in the legislation around the world from the 60s and 70s.

But this term describes in fact only one category of devices, and as the computer technology is developing, the usage of the term will be more and more unsatisfactory from a legislative point of view. On the other hand it is also not satisfying in penal legislation to supplement a new device in the statutes each time a quite different technological device is developed. In the technique of drafting penal legislation these difficulties have often been successfully overcome by adding for example "other means" or "similar" to a description or listing in the statutes. Such a supplement converts the question of the application of the statute to other means, devices or purposes than previously mentioned, to the courts, and it may sometimes result in unwanted burdens for the courts, followed by acquittals.

The use of "electronic devices" and "other means" or "similar devices" may of course still be the most suitable description, although not perfect.

Another approach to the problem of technological development of devices, is to turn the other way around and try to find a broader term, including all categories of devices today and of the future. With the variety of devices, such an attempt clearly involves the possibility of a too broad term also including manual or other unintended processing of data. Such a term is also introduced in the legislation, i.e. "automatic processing". Understood as "self-acting", in the meaning of a self-acting processing, this term is satisfactory in computer legislation, although it must be admitted the term "automatic" includes aspects of human behaviour. Another objection is that the term "automatic processing" also comprises other devices, for example electrical adding- or accounting-machines.

These objections can be avoided by supplementing or adopting a definition of "automatic processing". Such a definition is introduced in the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, approved by the Council of Europe in September 1980. Stated in this convention "automatic processing" includes the following operations if carried out in whole or in part by automated means: Storage of data, carrying out of logical and/or arithmetical operations on those data, their alteration, erasure, retrieval or dissemination.

In addition, also the OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, recommended September 23, 1980, use the term "automatic processing", but since these guidelines do not restrict themselves only to automatic processing of personal data, no definition was introduced.

In deciding which term to choose, great significance must be laid on these efforts. And the term "automatic processing" of data seems more flexible and applicable to what we may expect in the future development of devices. As to the objections, I would suggest the complete description of the protected devices in computer crime legislation as being "automatic data processing".

B. The model

a. Damage of data

"Whoever, unlawfully erases, modifies, affects or otherwise such damages data belonging to another, which are communicated, processed or stored by automatic data processing, shall be imprisoned not exceeding .... years, or fined not more than ..., or both."

1. The statute is aiming at everyone who is committing an offence as described. But important exceptions may be derived from the term "unlawfully". The perpetration must be in conflict with behaviour established in laws, or as widely accepted in many countries in conflict with behaviour derived from a common law point of view. The most important and practical exception from the two main principles are perpetrations with the consent or approval from the rightful owner of the data, making the act lawful.

   When the owner of the data is the employer, the employment's agreement or contract or given codes of ethics will regulate or advise the behaviour or acts of the employees. If not, the courts will evaluate the perpetrations in a case-by-case decision, whereby commonly accepted acts in the society or specific branch will be of importance, together with the interests of the owner of the data.

   A similar approach must be made when the perpetration is done by a party in contract with the owner of the data, for example a legal user.

The concept of the term "unlawfully" encompasses similar terms as illegal, dishonest, without authority, or without any colour of right.

Especially for the application on micro-computers of any kind, for instance personal computers for family or household purposes, data processed or stored in such devices must be included. Offences against such data will be evaluated to the same extent as offences against other property for family or household purposes. And in their rulings the courts will take into account the application of "unlawful" on such purposes, according to traditional juridical evaluation.

2. The protected "object" is data belonging to another. A definition of "data" is presented in Chapter I. But in the context of the purpose of this model statute, data processed by human beings are not included, only data processed or stored by automatic means, or communicated in a computer system. Data include all categories, also personal data, and as computer programs.

The data must belong to someone, of not, the perpetration does not constitute a criminal offence. And even data may in practice be abandoned, for instance atmospherical.

A more practical question is when data are owned by more than one. Normally the owners cannot erase or modify the data without an agreement or understanding with the others. If not, a perpetration constitutes a criminal offence according to the acts described in the model.

Another practical question is instances where the data have been made accessible to the public. Even if everybody can access a computer system and make use of the

data, someone, for example a government or an organization, is the owner of the data. And without the approval from the owner, concretely or publicly, a perpetration according to the model statute is a criminal offence.

3. The data must be communicated, processed or stored by automatic data processing. The meaning of automatic data processing is described earlier, but the functions cause some remarks.

The model legislation is aimed at encompassing offences against data from the moment they are entered at a terminal to the moment they appear at the same or other terminals, or other devices after having been communicated, processed or stored by automatic devices.

The term "communicate" includes the transmission of data to or within a central processing or storage unit, and the retrieval of data, including message switching capabilities[59] from one terminal to another, and all extended activities in the computer system other than the processing or storage activities, and in networks, for instance through switched circuits, hard wires and satellites.

Perpetrations as described in the statute will clearly be criminal offences, when intercepting data communicated

59. A message switching is the process of routing messages by receiving, storing and forwarding messages within a data network, e.g. the electronic mail, and the Electronic Funds Transfer System, including such networks as SWIFT, a telecommunication application in which a message received by a central system from one terminal is sent to one or more other terminals.

with processing or storage units[60]. In the computer technology of today, the erasure or modification of data communications can be accomplished with the necessary skills, knowledge and resources.

Data are "processed" by central processing units[61] (CPU), according to the individual specifications and capacities of the computer and the computer system. The term also includes the data processing of minicomputers and microcomputers (and as personal computers). In the latter small computers, the alternative "processed" in addition to storage functions appears the most practical, although data communications also occur.

Data can be "stored" by storage units[62] including the memory[63], and made available in the data processing or communications according to the individual specifications. Stored data may be erased or modified or affected to the same extent as the data are processed, but storage protections limiting access to a storage device will also limit the potential of criminal offences.

60. Some statutes concerning computer crime use the term "access". Without at the same time enacted interpretations in the legislation, it is unnecessary doubtful whether such a term applies on interceptions of data communications, for instance the Swedish Data Act, Section 21.

61. A processing unit is a unit of a computer that includes circuits controlling the interpretation and execution of instructions. Synonymous with central processor, main frame (ISO).

62. A functional unit into which data can be placed, in which they can be retained, and from which they can be retrieved (ISO).

63. Deprecated term for main storage (ISO).

4. The offence according to the statute is "erases, modifies, affects or otherwise such damages data". The listing of offences is aimed at typical acts in the computer environment.

   The erasure of data occurs when data and programs are obliterated from the original or previous legal appearance in their formalized manner. It may include one or many representations of facts, concepts or instructions from single information to a human being, to complete data bases and computer programs. The purpose of using the term "erases" includes the intentions when using similar terms as "obliterates" (The Swedish Data Act, Section 21) and "deletes" (the Californian Penal Code, Section 502, litra c). Only using the terms "damages" or "destroys" is too broad, the need for individualizing offences seems obvious, both from a preventive and deterrent point of view, and for the purpose of presenting the case to a jury or to the court.

   A criminal offence is constituted when a perpetrator, for instance without authority, directly from a terminal erases data, wipes out data and programs or parts thereof, or when the computer is programmed to erase one section of a file whenever a legal input occurs, or when erasure is made possible by intercepting data communications.

   Erasure of data occurs sometimes together with other intentions of the perpetrator. One of these is the alteration of data with destructive intent. Data or parts of data would be erased and replaced with other data, thus creating an alteration of the information to human beings, either understandable or as nonsense.

The destructive intent appears also by adding data to other data, without erasing data, resulting in changing the contents of data files or programs.

For the purpose of including both the latter destructive methods, resulting in the same appearance, namely the modification of the data, this term is chosen. In my opinion this term is preferable, although a broad interpretation of "alteration" is available, as used in some computer crime statutes.

Modification of data will constitute a criminal offence, for instance when a perpetrator alters a password or password files, other data or programs, or supplements data with destructive intent. This will also include for example inserting of data by creating obscene words, or altering grading files or programs in schools or universities with intent of destruction, or when destructive modification occurs through interception of data communication.

If not otherwise covered by erasure or modification of data, the automatic data processing can be destructed by other means, resulting in affecting the communication, processing or storage functions.

By automatic means the result or communication of the automatic data processing activity can be influenced. Many experienced cases have revealed that perpetrators are able to make the automatic data processing or storing inoperative - crashing the system - the result being closing down the computer or computer system for a short or extended period of time.

Other results by automatic means are causing the automatic data processing to process data at a slower speed, or cause the data processing to process incorrectly, or to omit correct processing.

Such acts affecting the automatic data processing constitute a criminal offence according to the statute.

5. The perpetrator must carry out the offence knowingly and wilfully. He must know that he erases, or modifies, or affects, or otherwise such damages data belonging to another, unlawfully or without a colour of right. If he wrongfully believes he has an authority or a consent from the owner of the data, no criminal offence results.

6. The offence should be regarded as a felony, minor offences as misdemeanours. In the evaluation of the damage done, one principle is essential. Data are assets of economic value. Data represent money directly, for instance in the Electronic Fund Transfer Systems (EFTS) or the international banking network SWIFT. Otherwise the loss of data can be measured in the cost of replacing or restoring, by the retail or trade market value, or a reasonable repair or replacement cost, of the damaged data. In addition a reasonable value of the damage created by the unavailability or the lack of utilizing the data or the automatic data processing should be emphasized.

b. Appropriation of data

"Whoever, unlawfully appropriates or obtains data belonging to another which are communicated, processed or stored by automatic data processing, shall be imprisoned not exceeding .... years, or fined not more than ...., or both."

1. The statute is aiming at everyone who is committing an offence as described. The term "unlawfully" causes the same exceptions as mentioned in the destruction of data. When the act is accomplished with the consent of the rightful owner of the data, or a party who legally disposes of the data, the perpetration is made lawful. Similar approach must be made in contracts and employees agreements, and in instances where the consent is not explicitly mentioned, but the act is widely accepted in the society or within the specific branch.

2. The question of ownership of data creates special problems in instances of appropriation or obtaining. The main juridical problem is whether data, or as information, are subject to ownership. It is argued that the meaning a human being assigns to the data is an intellectual "object" not suitable to the traditional juridical theory of ownership. From a philosophical point of view this is of course true, but when dealing with criminal realities, the Penal Codes in many countries are used to give means of punishment in order to protect "information", for instance in disclosure of information harmful to the operations of governmental institutions, or as trade secrets, although the methods of perpetration have only been verbal and without use of documents.

The approach to a solution in the automatic data processing must distance itself from this traditional juridical theory of ownership and property in the handling of physical objects. Instead the solutions must be based on the various elements in the concept of ownership, e.g. the responsibilities of production, use, security and maintenance.

There should be no disagreement that the value of data and databases, or as computer programs, are of such a category that unlawful appropriation or obtaining need the protection which a Penal Code can provide. In the statute this protection is given to the party to which the data belongs. The term "belonging to another" is based on the assumption that someone has produced the data, bought the data, or legally uses the data.

The data belong to the producer when they are developed for his exclusive use or for his purpose of trading them. This includes development by employees or consultants paid by the employer when his resources have been used in the production. Data, also as computer programs, developed during the course of business hours using the employer's resources, do not belong to the employee or the consultant. Common agreement should clarify exceptions from this main principle, but especially in regard to computer programs, programmers have no rights in programs written for employers, in absence of such an agreement. An employer has the right to expect no conflict of interest in the outside activities of an employee. On the other hand, if an employee has developed programs for his sole purpose or for other parties than the employer, using the employer's data or computer programs, or computer services out of ordinary business hours and during holidays, the product

is the employee's. However, using the employer's computer services without his consent constitutes unlawful obtaining of computer services. When data are traded, they belong to the party who has paid for the data or the development, in absence of any agreement.

If two or more independent parties have cooperated in the development of data or as computer programs, the same principle must apply. In absence of any agreement, the data belong to those who have ordered and paid for them.

Data, as computer programs, will often be legally used by other parties than the producer of the programs. In instances where computer programs belonging to one party are used to update another party's databases or data, the latter data belong to their producer. For instance, in a time-sharing system where the computer facilities, including computer programs are offered for leasing, the data and data bases updated for their own purposes belong to the lessee of the system.

3. The object of the statute is "data". But unlike the destruction of data, the act encompasses the transmission of the data to the terminal of the perpetrator, or to his computer system. The purpose of the act results immediately or later in knowledge when the data are transformed into information understandable to human beings. This information is the meaning that the perpetrator understands after the data are communicated to his terminal. It is the data, or in fact a copy of the data, which primarily are appropriated from the victim's computer, not the information. The data still remain as a collection of characters, which by means of

communication equipment and translation or transformation equipment are converted into knowledge and information to the perpetrator. Data are only potential information.

From a penal legislative point of view, at the time of perpetration, it is the data which are appropriated. The perpetrator's knowledge and information will eventually appear later on as a result of the perpetration. In one of the most prominent cases known so far, the U.S. von Seidlitz, see Chapter V, the defendant was able on his own terminal, by dial-up system, to obtain data representing a significant portion of a system program belonging to a federal agency in another state. It was the program itself that was valuable to him, not the information of the agency.

4. The offence according to the statute is "appropriates or obtains" data.

The appropriation of data, or as programs, occurs when data are accessed in the victim's computer system illegally and transmitted to the perpetrator's terminal. The act is fulfilled at his terminal, regardless of the data are transformed to information for human beings, or are the intended information or knowledge he was searching for. It may include one or many representations of facts, concepts or instructions, from single information to a human being, to data bases and computer programs. Only accessing the victim's computer system, not being able to transmit the data, constitutes only attempted appropriation, assuming that the intention was to appropriate the data.

Data are also appropriated when the victim's data communications are intercepted by means of "wiretapping" and the like.

The term "appropriate" includes both appropriations from outside remote terminals to the victim, and internal terminals in his computer system or network, for instance from employees or contractors, who illegally access data they are not authorized to access. When the latter groups have authorized access to the data, but use the data without authorization, it is only a question of unlawful disclosure of data.

The term "obtain" is intended for a broader application. It includes perpetrators who do not themselves access and appropriate the data, but acquire the data from others directly involced in the appropriation, or through another computer system, knowing the data are appropriated from the victim. Keeping and dealing with the data as they belong to him, is a violation of this statute.

According to this statute a criminal offence is constituted when a perpetrator unlawfully accesses the computer system of another and appropriates identification numbers, account numbers, passwords, personal data, financial data and the like, whether the data represent single information to the perpetrator or complete data bases or not. The statute also includes the appropriation of computer programs or parts thereof.

The means of obtaining or appropriating are indifferent. The intended means could either be reading the data on a terminal screen, or printed out at the terminal, or copying the data on disc or tape, and the like.

5. The data appropriated or obtained must be "communicated, processed or stored by automatic data processing". This includes data from the moment they are entered at a terminal or peripheral devices, to the moment they appear at the same or other terminals, and data generated or created in the computer without being input. The same remarks as mentioned in the destruction of data apply here.

6. The perpetrator must act knowingly and wilfully. He must know that he appropriates or obtains data belonging to another. If he wrongfully believes he has an authority or a consent from the party to whom the data belongs, no criminal offence results. Regardless of the intention was gaining himself or another, this will constitute an offence according to the statute.

7. Offences according to the statute should be regarded as felonies, and minor offences as misdemeanours. As with physical property or objects this distinction must be based on an evaluation of the data appropriated or obtained. Data can be evaluated either by quantity or by assets of economic value. Appropriating a vast amount of data may in some instances be of no harm or loss to the party which they belong to, and one or a few data items can be far more valuable than many large collections of data. Therefore, as with other statutes encompassing traditional property, the economic evaluation must be relevant.

   When merely appropriating or obtaining, in fact the copying of the data, this evaluation would be different from those concerning destruction or modification of data. The victim's data will still remain in his computer system, the only harm or loss is the exclusivity.

But also behind this exclusivity we can find an economic evaluation. The development of data, especially as computer programs or as data bases, will often be expensive to the producer or the party to whom the data belong. As time has passed in the computer technology, computer programs and data bases have been commercial products to be bought, sold and leased - retail and wholesale. In such instances the data can be measured economically either in the cost of production or in trade market value. If these values are not protected also by means of penal solutions, a potential of bankruptcy among such companies may occur rapidly as these industries are developing. In some instances the trade secret legislation serves satisfactorily, but in instances where the traditional requirement of secrecy is not fulfilled, or when such secrecy is not possible, a statute of appropriating or obtaining the data, including an economic evaluation of the products, is the only efficient remedy in penal legislation. The same approach must be made to parts of computer programs and data bases.

8. As mentioned earlier, the intention of this statute is to let it become a common vehicle against the unlawful appropriation or obtaining of data belonging to another.

Other statutes in penal legislation, protecting specific purposes, e.g. Trade Secret Acts, Copyright Acts, and the like, can be used either together with this statute or as independent statutes, according to the circumstances. But as such legislation has a tendency to be handled only as misdemeanours, and in addition has less applicability to many aspects of the computer technology, a common statute encompassing all appropriation or obtaining of data is preferable, especially from a preventive and deterrent point of view.

c. Obtaining computer services

"Whoever, for himself or another, unlawfully obtains services, using or making available a device, a collection of devices, or an interconnection of devices totally or partially belonging to another, which permits data to be communicated, processed, or stored by automatic data processing, shall be imprisoned not exceeding .... years or fined not more than ...., or both."

1. The statute is aiming at everyone who commits an offence as described. As with the destruction and appropriation of data, a consent from the party to which the device(s) belongs, makes the act lawful. Such a consent could be made explicitly, or in employments agreements, or in contracts. But also acts widely accepted, due to a common practice could make it lawful.

   When the services are made possible by a third party, for instance when the actual computer programs do not belong to the owner of the devices, a consent from the third party is necessary. Such a collision of interest may occur in time-sharing systems.

2. The object of the offence is a device, or a collection of devices, or an interconnection of devices. This is of course, in the language of today, the computer, the computer system, or the computer network. However, with the changing nature of technology and the concept of terms, I do not recommend the term "computer" included in the statutes. What we today understand with "computer" may not apply in the near future, having in mind the optical, biological and the like, processing of data.

In order not to exclude any new devices, and emphasizing the misuse of a device that permits automatic data processing, a more suitable term is using the term "device" itself. This term should be understood as synonymous to remedy.

These devices perform today what we describe as computer services, which is the affording of automatic data processing and storage functions, included more than one system with capability to transmit data among them through communication facilities. The devices must totally or partially belong to another than the perpetrator. In instances where devices belong to more than one, neither of them are allowed, in the absence of an agreement, to use them to the displacement or inconvenience of another.

3. The offence according to the statute is "obtains services, using or making available ..."

Obtaining services unlawfully occurs in the automatic data processing when a perpetrator without authority uses the devices after illegally having accessed the system, or employees or contractors using the devices to a greater extent than they are allowed to. These acts are often described as "theft of services" or "theft of time". The intention is either gaining his own purposes, or those of a third party.

The perpetrator must "use" the device of another. And the offence is fulfilled when a "job" not legitimated is started, or when the "service" afforded by the devices has begun, even if it is not revealed until some time has passed.

The term "making available a device ..." is aimed at instances where a person, for instance an employee or a contractor, is lending or leasing the device to another knowing the illegal purpose of the other.

The services must be obtained, encompassing the broadest understanding of procuring oneself an unlawful advantage, or causing or permitting some acts to be done.

Alle categories of unlawful obtaining of services will constitute a criminal offence according to this statute. This includes services for personal purposes as game-playing, processing of personal purposes, storing of personal files, unlawful communication, creating personal computer programs, creating subcompanies providing services to third parties, and the like. In fact, all purposes other than the purposes of the party to which the devices belong could constitute a criminal offence. It should be stressed that establishing loss or inconvenience, or deception, is not required. Such requirements are often difficult to prove, especially in the computer technology, and the purpose of the statute is aimed at the unlawful use as an independent preventive and deterrent effort.

4. The perpetrator must act knowingly and wilfully. He must know that he obtains services, using or making available device(s) belonging to another, and that he is not allowed to do it.

5. Offences according to the statute should be regarded as felony, minor offences as misdemeanour.

Both commercial time-sharing systems and time-sharing systems in governmental or scientific operations have put a monetary value on their computer services. Computer time can be estimated exactly in such systems. But also in instances of one-user systems these institutions, included all commercial activities, an economic evaluation mostly exist, due to the need of budgeting and other financial aspects of their computer services.

In events where a directly economic evaluation of services is not obvious, for instance in computers for more personal purposes, an evaluation of the unlawful time spent, or capasity problems, or the use of electrical power can be useful substitutes.

d. Modification of data

"Whoever, with fraudulent intent, alters or modifies data communicated, processed or stored by automatic data processing, which are destined to be used as evidence of a legally relevant matter of fact, or uses such data as true data, shall be imprisoned not exceeding .... years, or fined not more than ...., or both."

1. The statute is aimed at everyone who commits an offence as described. This is the modification of the data themselves and can be compared to forgery of documents. As with forgery, the result could be intended at establishing legally relevant matter of facts in otherwise legal transactions, for instance altering data later to be used in contracts, or resulting as a means of committing another criminal offence, for instance theft of tangible property or fraud.

   A consent from the other contractors, or the owner of the property in the latter group, does not constitute a criminal offence. When the modified data are used as a vehicle in fraud, the issue of consent is not a practical question according to the traditional requirements in fraud statutes.

2. The object of the offence is the data communicated, processed or stored by automatic data processing. It involves the modification of data from the moment they are entered into the system at a terminal to the moment they again appear at the same or other terminals. The most practical modifications are directed at processed or stored data, but the data could also be modified while in transit from a central processing unit to a

terminal, or between two terminals. The discussions involve the same questions as with the destruction of data, see page 95, but unlike the modification with destructive intent, the offence according to this statute is aimed at the fraudulent intent.

3. The offence according to the statute is "alters or modifies" data. The alteration of data occurs when data, also as programs, are changed or replaced with other data from the original or previous legal appearance in their formalized manner. The offence assumes the erasure of the previous data, replacing them with new data, and thus alters the valid concept of those data, the result intended to be understandable to human beings after having been transformed.

   The fraudulent "modification" of data occurs as an independent alternative in instances of erasure without replacing the data, and the adding or supplementing of data to the original or previous state, thus changing their concept.

   Both the fraudulent alteration and modification of data would most practically be perpetrated from a terminal directed at the existing data in the system, but the statute encompasses also instances where the discs and tapes, and the like themselves are replaced by substitutes contaning false data wholly or partially.

   A criminal offence will be constituted when a perpetrator, for instance with fraudulent intent, changes personal or financial data, making false data entry, deleting data, and the like.

4. In the first alternative the data must be "destined to be used as evidence of a legally relevant matter of fact". As with forgery of documents this requirement is aimed at establishing legal transactions or dispositions, and the evaluation must be similar.

   The alteration or modification of data must constitute a legal obligation or liability, depending on the result of the offence.

5. Another alternative in the statute is "uses such data as true data", thus altered or modified. This encompasses all categories of acts where the altered or modified data are used. The usage of such data appears when the perpetrator himself is using the data in legally relevant transactions, but more important is using the data as a remedy in other categories of crime, for instance fraud, theft and embezzlement involving tangible property. Using altered or modified data in the latter categories is an independent criminal offence, and this statute is aimed at being used in conjunction with such more traditional statutes.

6. The perpetrator must carry out the act knowingly and wilfully. He must know that the data are false data, altered or modified. In the event of making use of them, he must know that he uses the data as true data.

   The purpose in both instances must be aimed at defrauding another.

7. Offences according to the statute should be regarded as felonies. Unlike the other statutes, altering or modifying data resulting in change of only one single data item may constitute a severe problem to another party or his operations. The distinction of a minor offence, eventually resulting in misdemeanour, is not obvious in the offences this statute is dealing with.

SECTION VII: CONCLUSIONS FOR NORWAY

In addition to the following special computer crime legislation for Norway, which will be printed in Norwegian only, I recommend a thorough evaluation of the existing statutes in the Norwegian Penal Code. Statutes which are not necessarily related to the automatic data processing must be updated also addressing the aspects of computers.

Mine forslag til straffebestemmelser om datakriminalitet inntatt i straffeloven er som følger:

§1: Den, som uberettiget sletter, endrer, påvirker eller på annen måte slik skader data som helt eller delvis tilhører en annen, og som er bearbeidet, lagret eller i kommunikasjon ved automatisk databehandling eller automatiske hjelpemidler, eller medvirker hertil, straffes med bøter eller fengsel inntil 3 år eller begge deler.

Er skaden grov, settes straffen til bøter eller fengsel inntil 6 år eller begge deler. Medvirkning straffes på samme måte. Ved avgjørelse av om skaden er grov, skal det særlig legges vekt på om skaden er betydelig, om den skyldige vitende har voldt fare for noens liv eller helbred, eller om skaden er voldt på offentlig eller for allmennheten automatisk behandling eller kommunikasjon av data.

§2: Den, som uberettiget tilegner eller erverver seg data som helt eller delvis tilhører en annen, og som er bearbeidet, lagret eller i kommunikasjon ved automatisk

databehandling eller automatiske hjelpemidler, eller medvirker hertil, straffes med bøter eller fengsel inntil 3 år, eller begge deler.

Er tilegnelsen eller ervervelsen grov, settes straffen til bøter eller fengsel inntil 6 år, eller begge deler. Medvirkning straffes på samme måte. Ved avgjørelsen av om tilegnelsen eller ervervelsen er grov, skal det særlig legges vekt på om gjerningen gjelder en betydelig verdi eller av andre grunner er av særlig samfunnsskadelig art.

§3: Den, som for seg selv eller andre uberettiget bruker eller forføyer over hjelpemidler i automatisk databehandling som helt eller delvis tilhører en annen, og som tillater kommunikasjon, lagring eller bearbeidelse av data, eller medvirker hertil, straffes med bøter eller fengsel inntil 3 år, eller begge deler.

Er den uberettigede bruk eller forføyning grov, settes straffen til bøter eller fengsel i inntil 6 år, eller begge deler. Medvirkning straffes på samme måte. Ved avgjørelsen av om bruken eller forføyningen er grov, skal det særlig legges vekt på om det voldte tap er betydelig, eller om gjerningen har påført den berettigede betydelig ulempe.

§4: Den, som i rettsstridig hensikt endrer, innfører eller sletter data bearbeidet, lagret eller i kommunikasjon ved automatisk databehandling eller automatiske hjelpemidler, og som er bestemt til å tjene som bevis for en rett eller en rettslig relevant disposisjon, eller medvirker hertil, straffes med bøter eller fengsel inntil 3 år, eller begge deler.

Benyttes slike data som ekte, til middel ved forøvelsen av en forbrytelse, settes straffen til bøter eller fengsel inntil 6 år, eller begge deler. Medvirkning straffes på samme måte.

§5: Den, som forøver eller medvirker til slik gjerning som beskrevet i §1, 1.ledd; §2, 1.ledd og §3, 1.ledd, straffes med bøter eller fengsel inntil 6 måneder, når straffeskylden må regnes for liten på grunn av ubetydelig skade, tap eller ulempe i den automatiske databehandling, og forholdene forøvrig. Medvirkning straffes på samme måte.
(Bestemmelsen bør inntas i kapitlet om forseelser.)

APPENDIX A

A MODEL COMPUTER CRIME LEGISLATION

SECTION 1: DAMAGE OF DATA

"Whoever, unlawfully erases, modifies, affects or otherwise such damages data belonging to another, which are communicated, processed or stored by automatic data processing, shall be imprisoned not exceeding .... years, or fined not more than ...., or both."

SECTION 2: APPROPRIATION OF DATA

"Whoever, unlawfully appropriates or obtains data belonging to another which are communicated, processed or stored by automatic data processing, shall be imprisoned not exceeding .... years, or fined not more than ...., or both."

SECTION 3: OBTAINING COMPUTER SERVICES

"Whoever, for himself or another, unlawfully obtains services, using or making available a device, a collection of devices, or an interconnection of devices totally or partially belonging to another, which permits data to be communicated, processed, or stored by automatic data processing, shall be imprisoned not exceeding .... years or fined not more than ...., or both."

SECTION 4: MODIFICATION OF DATA

"Whoever, with fraudulent intent, alters or modifies data communicated, processed or stored by automatic data processing, which are destined to be used as evidence of a legally relevant matter of fact, or uses such data as true data, shall be imprisoned not exceeding .... years, or fined not more than ...., or both."

APPENDIX B

CATEGORIES OF RELEVANT COMPUTER CRIME

The following categories of computer crime are relevant to the purpose of this document. They include cases from the SRI-International files, and reports from the member countries of Interpol. The cases are evaluated and presented by the author of this document. In order to avoid unintentional identification of perpetrators and victims, the cases are presented as anonymously as possible, and all amounts of money are estimated in U.S. dollars.

A. DAMAGE OF DATA

Case 101 A large commercial company in USA with worldwide access to its computer systems through international telecommunications networks discovered in 1980 that they had some serious problems in their systems. Somebody was erasing files, creating files, modifying files by inserting pornographic words, and bringing the system down. The company soon found out that the attacks were from outside remote terminals. To publish the fact that the systems had been compromised, the attackers also broadcast several obscene messages to system users. One group of users received the following message from the attackers:

> "The phantom, the system cracker strikes again, soon I will zero your disks and your backups on system A. I have already crashed your system B. Have fun trying to restore it you ....."

The company by telephone instructed users to change their passwords, but it was useless because the attackers had been able to establish privileged accounts of their own in the system. To keep the attackers off the system, the company had to shut the system down, examine all disk files for anomalies, recreate the disk system, and regenerate the operating system. This remedial activity caused the system to be unavailable for almost two days. The company estimated the total cost associated with the series of incidents which went on for three days, to a loss totalling $150.000. After satisfactory security measures were established and the case reported to the police, the perpetrators were caught. It was then discovered that they had used a home computer (micro computer) programmed to emulate a computer terminal in accessing the

company's computer system from a remote terminal. The telephone number needed was obtained by automatic scanning, using the micro computer. The perpetrators were convicted under the Californian Computer Crime Law, but the company was still receiving until a year later, attempted attacks by other attackers on the average of once per week. It is suspected that the information about how to compromise their systems was circulated through electronic bulletin boards all over the United States.

Case 102 (SRI 81405) B) Two high school students in USA compromised the school district computer system. They obtained user accounts, and from their terminals they checked for interesting file names that were marked not secure and privileged mode. After having succeeded in finding one, they overwrote their own program and had a privileged mode program to execute. It dumpted the password file and gave total system access. The students crashed the system several times.

Case 103 (SRI 81402) A group of students at a university in USA compromised the university computer system. The students uncovered a special "super user program" and changed the program's password to give them access to all accounts on the system. They denied computer center operation personnel access to the system, and wiped out the system's billing file for most of a month. The system had to be shut down for three days following the incident in order to regenerate it, using a new password. The students were caught after the computer personnel examined computer account records and uncovered

their suspicious activity. After the incident the computer center is sending a stern warning to all users that further security breaches will not be tolerated.

Case 104 (SRI 81405) A) A high school student in USA accessed the district school's computer center via dial-up telephone system, mostly from his home terminal. He altered files and the teachers' grading program. In trying to bring the digits back to the previous status, the system crashed and brought down the entire system, destroying more than a week of work by the district data center staff and delaying grades and paper work for another week.

Case 105 (SRI 78212) An employee dismissed from a small company in USA expressed his annoyance with the company by programming the computer to erase a section in the memory bank whenever there was an input including the back-up copies. Two weeks after the employee left, the company discovered there was nothing in the computer system.

Case 106 (SRI 77408) A 15 year old high school student in USA accessed the district school computer center and wiped out programs and data, and inserted obscene words over a period of two-three weeks.

Case 107 (SRI 77110) Three keypunch operators at a State Department of Justice deleted arrest records of about 75 persons over a period of one month from the criminal history system in a governmental computer system in the USA. The erasure was accomplished from the terminals where they were assigned.

Case 108 From terminals at their high school in USA four 13-year old students were able to access a computer in Canada and destroy data and programs through the telephone dial-up system. The students had received extensive instructions in computer technology and used their experience in at least 41 telephone calls in 1980 to access or attempt to access 20 user files in a large Canadian time-sharing company involving several Canadian companies and universities. After several trial and error attacks, they were able to gain access to victims' files or parts of files. Back-up copies were available, so disruption and loss of time were small, but in one victim's files they erased 1/5 of the data. It was assumed that they obtained the correct telephone number from another source. The police got involved, and the telephone calls were traced to the school in USA where the students were caught through a sophisticated investigation scheme. The case was not prosecuted because they were juveniles.

Case 109 Interpol A disgruntled employee of a printing company using a computer word processor, erased part contents of a book awaiting printing, causing damage valued at $ 3000.

Case 110 Interpol A programmer using a remote terminal accessed his previous employer's computer data center 30 miles away and corrupted customer files. When interviewed, his excuse was that as he had originally programmed his previous employer's computer system, he expected to be invited to assist in correcting it.

Case 111
Interpol

A university had some of its stored data on their computer systems corrupted and damaged by a group of students using remote computer terminals 240 miles away.

Case 112
Interpol

Tapes containing information relating to welfare payments to be made by a governmental institute were erased deliberately by a disgruntled employee, working in the institute's computer center.

Case 113
Interpol

Four software company employees were altering library and storage programs, rendering them usable when they left the company. They set up their own software company and marketed the storage programs themselves.

B. APPROPRIATION OF DATA

Case 201 (SRI 81403) A 15-year old student and several adults accessed computer systems of many companies across USA, attempting to appropriate data from terminals and through telephone dial-up systems.

Case 202 (SRI 81406) Three students and a former student at a university in USA obtained other students' account numbers and passwords to gain access to data stored in the computer system. In some cases the students have tapped into another's account, received a print-out of the data they wanted, and then intentionally crashed the system to destroy evidence linking them to that specific account.

Case 203 (SRI 80402) A police officer in USA was selling cocaine on the side. In order to know whom he was dealing with, he used his position as a trusted employee to gain access to the U.S. Department of Justice criminal history data base to obtain possible criminal violent records of the buyers of cocaine. He appropriated the confidential data from a terminal which was linked to the Department of Justice's computer system.

Case 204 (SRI 79406) A police officer in USA working on the side for private detective agency, used his position and accessed and obtained data on the people he was investigating for the private agency. He was discovered after a person complained that the officer had investigated him in a divorce case.

Case 205 (SRI 78213) An employee of an airline company in USA copied a computer application program on discs he had helped to develop. He formed his own company while still working for the airline company, using his employer's computer services and other employees to prepare the program. He sold two copies of it without paying royalties. The employee argued that the program was not "property", but a "concept or idea" in his mind. Hence, he argued, the act was not theft but non-criminal duplication. The court did not agree with the argument and established the offence as theft. The investigators determined that no copyright or trade secret violations could be found. The original damage was assessed at $ 15,000, equal to the price of the programs he sold, plus $ 900 equal to the usage of keypunch time. These estimations were later reduced to $ 30 for a disc and one cent per keypunch card.

Case 206 (SRI 78218) A programmer previously employed by a computer service bureau in USA was convicted of copying his former employer's computer programs. Although no conclusive evidence was presented, proving the defendant had in fact duplicated the programs, a jury found enough circumstantial evidence to convict him. It is alleged that the jury made its decision largely on the basis of expert testimony that stated it would be impossible to recreate the programs so precisely in the short amount of time that elapsed between the time the defendant left his former job and the time he started his own company. The defendant had throughout the trial argued that he had originally developed the programs, and that he had recreated

rather than copied them once he left the former employer, and he appealed the conviction.

Case 207 (SRI 77216) Two county employees in U.S.A. attempted to obtain data from a police department computer file they were not authorized to use. They used their own codes and were discovered when a police department employee realized the person making the request from a terminal was not authorized to see that particular data.

Case 208 (SRI 76208) A county computer operator in U.S.A. appropriated computerized assessment data allegedly by having the data copied on a tape and then sold the tape. An unauthorized computer time was discovered in a review of the governmental bureau's internal control procedures.

Case 209 (SRI 75218) A former employee of a computer service company in U.S.A., who had supervisory authority for technical conversion and operation of a data center under contract to several federal agencies, was able, on his own terminal in another state via telephone connection, to obtain account numbers and other information which were necessary for him to access the computer systems exclusively used for the governmental agencies. Having access to this system, he obtained data representing a significant portion of a system's program. It was the system's program itself that was valuable, not the information of the federal agency. The perpetration

was discovered by an employee in the company, who noticed that the ocmputer was in use on an identification number belonging to a colleague, who was present and did not use the terminal.

Case 210
Interpol

An employee of an international car-hire company obtained a printout of the customer list stored in the company's computer and sold it to a competitor. As in that country's legislation information cannot be stolen, he was charged with theft of the printout paper.

Case 211
Interpol

A computer system of a company in a country was violated by someone in another country. Entry was gained but nothing was changed or erased. Security measures were changed to eliminate the problem before investigation commenced.

Case 212
Interpol

A computer technician working for an insurance company used his terminal screen to consult a file on car insurance which had nothing to do with his work. Caught in the act, he admitted he intended to use the information for his own benefit, and it was also established that he had taken away a computer printout. He was prosecuted for the theft, and sentenced to imprisonment for two months, suspended for three years. He was prosecuted for theft, and found guilty only of fraudulently removing a "listing of undetermined value".

C. MODIFICATION OF DATA

Case 301 (SRI file) An individual employed by a governmental institution in USA applied for a loan at his credit union. In the application he listed all of his outstanding debts. His loan application was denied on the basis that there were two loans that he had received that were not shown on the application provided to the credit union. When the individual asked what the two loans not listed were for, he was told that they were for purchases made in another city in the same state. The individual thought this quite strange because he had never heard of the companies shown, nor had he recently transacted any business in the other city. The unexplained amounts owed totalled $ 2900 at the time of the inquiry, and he asked the credit data company for a copy of his credit history file.

After receiving a copy of this file he noticed that his address was listed as being in the other town, and his own address was shown as a former address. Further inquiries revealed that a person by the same name as his own was living at this new address. This person explained that he had a bad credit record, and that a friend had offered to improve his credit for a fee. The friend had gone to some group of persons that scanned the state for another individual with the same name and with a good credit history. The group then apparently accessed the credit data company's credit history data base, and changed the address of the individual. This was relatively easily done due to the fact that the policy of the company was to make their system

easy to use so that merchants would be able to carry on business with the least interference.

After receiving this information the credit data company corrected the individual's credit history. At the bottom of this new credit history is a notice that says: "This individual's credit history has been used without his consent to obtain credit by persons unrelated to the individual. Each time that this record is used it is requested that a confirmation by phone be made with the individual."

Case 302 (SRI 81203) An air traffic controller in USA pulled a prank on his colleague by entering less than 20 phony flight plans into the installations air traffic control system. The plans apparently consisted of a series of fake air craft numbers, which the controller allegedly entered at his terminal keyboard. The numbers were soon displayed in a tabular list on a fellow air traffic controller's radar screen, where the flight plans were quickly found to be sham.

After the suspicious flight plans were proven to be false, they were rapidly traced to an on-duty air traffic controller, who was immediately removed from service.

Case 303 (SRI 80406) A records supervisor at a police department in USA made a false entry into a national computer information system, that a relative of hers was wanted on a charge of auto theft. The relative was detained on the charge in another state within the next couple of days.

Case 304 (SRI 80203) In a city in USA a routine audit of the city's traffic violations bureau revealed that more than 170 unpaid parking tickets in the computer system were erased or altered, most of the tickets issued to half a dozen data processors who were employed to operate the computer system. It was discovered when an auditor compared a sample of several hundred of the 60,000 actual tickets in the bureau's files against the computer log and found that one ticket in the bureau's files had been "cleared" on the printout, indicating the fine had been paid. Because the ticket was voided with a different code than that routinely used when a fine is paid, the auditor searched the system for other tickets cleared with the same code. The computer turned up more than 170 issued over a 15 to 18 months period in an area near the computer center. The actual paper files indicated the tickets still were "open".

Case 305 (SRI 80209) An air traffic controller at an airport in USA removed air traffic control data on an incoming airliner from the computerized radar scopes at the airport. The incident resulted in that the flight was flying about 6 miles at the wrong altitude in the normally crowded skies over this specific international airport. The alphanumeric data describing the airliner's radar "blips", flight name and number, altitude and ground speed were deleted.

Case 306 (SRI 78202) Two students at a university in USA accessed the university's computer system and attempted to alter their grade records and financial aid status by accessing the system to award themselves good grades and credit for courses not taken. The students also tried to access the registrar's financial aid files in order to change their need status, which is based on personal or parents' income. If successful, they could have received unwarranted financial assistance.

Case 307 (SRI 75210) An employee of a computer company working for a police department in USA was angry with his wife, so he programmed the computer to report that her car had been stolen, knowing she was driving it. The wife got picked up.

Case 308 (SRI 77404) One group of classmates with computer education pulled a prank on their fellow students at a neighbouring rival school in USA. The group of students were able to access the school district computer system from their terminals, obtained the district computer report card forms by some means, and printed out grades for all seniors at the rival school, giving them "F" in every subject. At the same time all seniors in their own class received straight "A" on their report cards. Parents of the latter students were reported to be overjoyed, and gave their children privileges they would not normally get. The other parents were not happy at all when they received the reports in the mail, until they were convinced it was a joke.

Case 309 (SRI 77213) A student at a university in USA, working for the university as a computer operator, altered grades for himself and fellow students by changing data stored on computer discs. In one incident he altered 22 grades for one student, receiving approximately $300, and in another incident altered 11 grades, receiving $100.

Case 310 (SRI 76335) A former employee in a credit bureau in USA upgraded computerized credit ratings for an estimated 30 people. It resulted in as much as $200,000 in bad loans and credit card purchases for banks and businesses.

Case 311 (SRI 76211) Twelve employees at a university in USA, who had access to the university's computer center and/or the registrar's office, were implicated in a grade-changing conspiracy in order to upgrade their own transcripts or the transcripts of friends or relatives. They were accused of changing a total of 69 grades of 13 students' records. The scheme was discovered when a student transcript that showed graduate eligibility was disproven after the student's professor denied giving out the grade record for one of the courses, and an audit was initiated.

Case 312 (SRI 76213) Three employees of a nationwide private clearing house for credit records in USA altered credit histories in the company's data banks to improve individuals' credit ratings, who illegally paid $450 to $1500, totalling at least 300 people. The changes were made from a terminal where one of the perpetrators worked, and it resulted in

a huge amount of bad bank loans and credit card purchases.

Case 313 (SRI 75403) A police chief in USA was indicted for tampering with government records. He was accused of having deleted reckless-driving offence from his record in the county's regional computer system.

Case 314 Interpol A soldier in an Army Pay Corps, working as a computer operator, caused a defamatory statement to be printed on the chief of staff's pay sheet by the computer.

Case 315 Interpol A bank in a country received a magnetic tape through the mail. The tape contained instructions from a major customer to transfer $3,000,000 to various bank accounts. Due to a difference in the pulse rate on the tape leader with the identification code, investigations were made, and the attempted scheme was discovered. It revealed that the tape had not been prepared by the customer, and the accounts involved were opened with false identities.

D. OBTAINING COMPUTER SERVICES

Case 401 (SRI 81404) A student at a university in USA used his terminal at one of the university's institutes to gain access to computer systems at other universities elsewhere in the state. Through a dial-up system he was able to communicate with the other universities' systems by unauthorized routing his phone calls through intermediate campus computing centers. The unauthorized service was also used to play games like "Dungeons and Dragons" and "Star Trek" with students at the other universities. An internal audit uncovered some 45,000 minutes of unauthorized computer use and more than $7,000 worth of illicit long-distance telephone bills. It was estimated that most of this misuse could be directly attributed to the student. After his arrest the police confiscated a three-foot high stack of printouts containing suspicious messages from students around the country.

Case 402 (SRI 81409) A computer programmer, employed by a board of education in USA set up a race-track betting system, created programs for the benefit of his own horse farm, in addition to using the board of education computers to trace the genealogies of his horses back seven generations.

The unauthorized use was discovered after a directive from a city government to the heads of city agencies to order their employees to "remove immediately all unofficial data files and programs from city computer systems".

The Criminal Court judge dismissed the theft of service charges against the programmer. The judge ruled that whatever the computer specialist might or might not have done, he had not broken the law because he had legitimate access to the equipment. "It was not the intent of the Legislature to forbid unauthorized internal use of equipment, but rather unauthorized use of equipment in a commercial setting where the equipment or service is being leased for hire," the judge stated. The judge suggested, however, that with the profileration of computers, word processors and other electronic equipment, the Legislature might wish to consider regulations governing a broad array of abuses that have become possible.

Case 403 (SRI 81401)

Two directors at an institute of technology in USA were able to set up a data storage company within the institute's computer system. They served three business concerns, a medical magazine subscription company, an aircraft parts company, and an import-export company. They illegally used more than $200,000 worth of time on the computer, and the three private companies paid at least $40,000 in fees to the directors. Telephone lines were installed and tied into the institute's computer for use only by the data storage company clients. The usual access procedure to the institute's computer system was changed slightly, so that the institute's name was not mentioned, allowing the clients access. The crime was discovered when officials at the institute noticed that an increased amount of disc storage was being used, and the institute's computer was noticeably less productive.

Case 404 (SRI 79404) In USA an internal investigation at a governmental research center revealed that more than 200 employees had stored 456 unauthorized files for personal purposes in the time-sharing system used by the research center. Some of the employees were also connected to the computer system through dial-up telephone system from terminals at their homes. The files included several hundred games, such as "Star Trek" and the like, poetry, jokes, personal letters, a beer collection catalogue, etc. One of the employees had even used the computer system to assist local gamblers run a bookmaking operation. The investigators found that a common practice at the research center was to share passwords among staff people. Also, passwords were changed only once a year, so that a person leaving the center could still access the computer system, using another person's password. Following the investigation, the research center issued a policy directive stating any use of a facility computer must be for official work.

Case 405 (SRI 79405) For more than a year a 15-year old high school student accessed computers at a nearby university computer center in USA without authorization. From a terminal at his home and through dial-up telephone system he used the computers for at least 200 hours of computer time worth an estimated $10,000, in addition to disrupting some of the university's computer operations. Because the university tried to make its computer facilities as "friendly" and available as possible, an authorized user could gain access to the systems relatively easily. The unauthorized use was

discovered when employees at the university noticed a long series of hitches that hindered operations in the computer center. Hardware began to experience an unusual amount of down-time. Data was inexplicably lost, and users - from among both the university's faculty and its student body - suddenly found themselves unable to run necessary programs.

Case 406 (SRI 79408) A private consulting firm was the legal user of a computer service company in USA, which also served several other clients in a time-sharing system. The firm normally gained access to the computer system by dial-up system, using a code which also was used by the computer service company to bill clients for time used.

However, the firm learned the codes of other clients of the computer service company, and manipulated the computer to charge those clients for computer time it used for itself or its own clients. It enabled the firm to charge its clients less to provide services, because they were being subsidized by other unsuspecting clients of the computer service company. The consulting firm got the unauthorized computer codes because it had done work for the other clients of the computer service company in the past, or because of loose security by those clients.

The perpetration was done after the consulting firm entered the computer through its own code and switched to another client's code in the time-sharing system while its computer terminal

was tied to the computer by dial-up connection. When it finished running work on the other client's account, it switched back to its own account before hanging up. The strategy was making it look like the consulting firm finished its work, then the other client came on-line, then the consulting firm tapped the computer again.

The scheme was discovered when one of the clients complained about unusual high bills, and the computer service company initiated investigation.

Case 407 (SRI 78403) Two students gained access to a computer system at an institute of technology in USA, after illegally obtaining identification codes. The students used a remote terminal at home and an on-campus terminal in a dial-up system. They used the computer system without authorization over $200 worth of computing time, playing games such as "Dungeons and Dragons" and "Star Trek".

Case 408 (SRI 78404) A computer operator at a university in USA twice accessed a computer system at a university in another state without authorization. He used the time to play computer games, as well as breaking a security code that allowed him to tap into a secret data bank reserved for the university's officials.

Case 409 (SRI 77401) Two computer programmers in a large computer manufactory company in USA developed over a three years period a computer program able to revise music into digitized form, selectively edit music, and print out any desired format.

They used their employer's computer in the development, totalling $144,000 worth of computer time.

They set up their own company in order to sell the products, and used the mail in advertising and trading. Because of the latter acts they were convicted for mail fraud, in addition to conspiracy, and not for unlawful use of the employer's computer.

Case 410 (SRI 77409) One former employee of a research institute in USA and an employee of a company responsible for maintenance on the computer system at the research center, used this computer system for their own established company without authorization.

It was discovered by one of the supervisors at the research center, who noticed several directories were still in active use, even though the individuals to whom they had been assigned had left the organization. When the supervisor reviewed the data in the files, he found data pertaining to the formation of an electronics manufacturing company. The estimated unauthorized use was valued at about $2,000 worth of computer time.

Case 411 (SRI 77411) Three students at a university in Canada accessed the university's computer system from terminals in another building, linked to the system over telephone lines. They were able to establish unauthorized accounts for themselves by altering the account records, and reserved portions of the memory for their own use.

The unauthorized use, totalling a vast amount of time, went on over a period of several months. In addition, the system was crashed several times and their activities caused severe damage and inconvenience to legal users.

Case 412 (SRI 75401) An individual was able to copy a valid account number and password accidentally left out by another user at a university in USA. He used the computer system at the university for his own purposes, totalling at least $1,700 worth of computer time over a period of three weeks.

Case 413 (SRI 75404) An employee at a university in USA used the university's computer system without authorization to print campaign material in a public school election. He used a terminal installed in his home programming the computer through dial-up telephone system, and received printouts of the campaign material at his terminal.

Case 414 (SRI 75406) A former employee of a computer manufacturing company in USA with worldwide network to their representatives, went to work for a company which became a customer to the former employer. With knowledge of the passwords belonging to various representatives in other countries, he made a vast amount of accesses to his former employer's computer system, using it for 143 hours, totalling $15,000 worth of computer time. He claimed he was using the system for the benefit of his new employer, although he made illegal use of the representatives' passwords. It was discovered

when the former employer's representatives in London and Paris noticed that they were being billed for time they did not actually use the computer.

Case 415
Interpol

A data processing manager and a programmer employed by a local authority, used their employer's computer without authorization. They had conspired together to form their own computer company, and then used their employer's computer to do accounts work for outside companies.

Case 416
Interpol

A large-scale betting took place among some senior staff members of a corporation during the national baseball championship tournament of a country's senior high schools. A computer system owned by the corporation was used without authorization for the calculation of bets and shares.

Case 417
Interpol

A micro-computer company arranged a computer class, to which a professor at a university was invited as an instructor. During the instruction a salesman of the company obtained from the professor the passwords which were used for operating the computer at the university. After that time the salesman accessed the university's computer system through the use of the passwords and used the system without authorization whenever he performed instructive demonstrations in similar classes.

APPENDIX C

BIBLIOGRAPHY

Bequai, August: Computer Crime, Lexington, Massachusetts, D.C. Heath, 1977.

Bing, Jon and Selmer, Knut S. (ed): A Decade of Computers and Law, Universitetsforlaget (Publishers to the Norwegian universities), 1980.

Bloombecker, Jay: The Investigation of Computer Crime, National Center for Computer Crime Data, U.S.A.

Computer Crime - Criminal Justice Resource Manual, National Criminal Justice Information and Statistics Service, U.S. Department of Justice, 1979.

Computer Crime - Legislative Resource Manual, Bureau of Justice Statistics, U.S. Department of Justice, 1980.

Computer Security in Federal Programs, Committee on Government Operations, United States Senate, 1977.

Coughran, Edward H.: Computer Abuse and Criminal Law, University of California, San Diego, 1976.

EDP and the Vulnerabilities on Society, Department of Defence, Sweden, 1978.

Gammer, Michele A.: Computer Crime, American Criminal Law Review, Volume 18, Number 2, American Bar Association, 1980, page 370 - 386.

Parker, Donn B.: Crime by Computer, New York, Charles Scribner's Sons, 1976.

Parker, Donn B.: Ethical Conflicts in Computer Science and Technology, AFIPS Press, Arlington, Virginia.

Schjølberg, Stein: Computer-Assisted Crime, the Norwegian Research Center for Computers and Law, University of Oslo, (Norwegian text only), 1980.

Schjølberg, Stein: Computer Crime in Norway, a Decade of Computers and Law, page 440 - 459, Universitetsforlaget (Publishers to the Norwegian universities), 1980.

Schjølberg, Stein: Computer-Assisted Crime in Scandinavia, Computer/Law Journal, Vol. II, No. 2, page 457 - 469, U.S.A. 1980.

The Investigation of White-Collar Crime: A Manual for Law-Enforcement Agencies, LEAA, U.S. Department of Justice, 1977.

Tapper, Colin: Computer Law, Longman Group Ltd., London, 1978.

Whiteside, Thomas: Dead Souls in the Computer, The New Yorker, August 1977.

Bigelow, Robert P.: The Queen v. McLaughlin or Why the Criminal Sometimes Goes Free, Computer Security Journal, Spring 1981.

Other Publications in the CompLex series

CompLex 1/81
Johs. Hansen:
A Computer System for Analysis of Legal Decisions

CompLex 2/81
Johs. Hansen (ed.)
Papers on Deontic Systems

Complex 3/81
Vidar Sørensen:
Information Systems etc. for Norways Geotechnical Institute

CompLex 4/81
Kjetil Johnsen:
Systemtechnical Consequences of Personaldata Legislation

CompLex 5/81
Marit Thorvaldsen:
Veiwdata and Legal Information

CompLex 6/81
Anne Kirsti Brække:
The Mail Monopoly

CompLex 7/81
Knut S. Selmer (ed.)
The LAWDATA Papers
English only

CompLex 1/82
Nordic Data Protection Legislation
Council of Europe Convention
OECD Guidelines

CompLex 2/82
Harald Brænd and Vidar Sørensen
Oil Spill Protection: User Needs and Sources

CompLex 3/82
Jon Bing and Dag Frøystad
User Studies of Legal Research
NORIS(48)

CompLex 4/82
Thomas Prebensen Steen
The Regulatory Liability of Post- and Telecommunication Services
With a summary in English

CompLex 5/82
Annual Report (1981) of the Norwegian Data Inspectorate

CompLex 6/82
Bing/Eckhoff/Frøystad/Oskamp
CATTS: Computerized Program for Teaching Text Retrieval Systems

CompLex 7/82
Jon Bing
Information Systems for the Social Security Court. Legal Communication Processes.

CompLex 8/82
de Mulder/Oskamp/van der Heyden/Gubby
Sentencing by Computer: An Experiment

CompLex 9/82
Colin Tapper
An Experiment in the Use of Citation Vectors
in the Area of Legal Data

CompLex 1/83
Arve Føyen
Report on Amendments in the Norwegian
Data Protection Legislation

ISBN 82-00-06570-7