UIC John Marshall Journal of Information Technology & Privacy Law

Volume 2
Issue 1 *Computer/Law Journal - 1980*

Article 22

1980

# Computer-Assisted Crime in Scandinavia, 2 Computer L.J. 457 (1980)

Stein Schjølberg

## Recommended Citation

Stein Schjølberg, Computer-Assisted Crime in Scandinavia, 2 Computer L.J. 457 (1980)

# COMPUTER-ASSISTED CRIME IN SCANDINAVIA

*by Stein Schjølberg*[*]

## INTRODUCTION

Electronic data processing (EDP) has revolutionized our society almost unnoticed. Most public and private institutions, companies and organizations have already put EDP into practice, or are considering doing so. What is happening in our society can only be designated a technological revolution.

There has been enormous technical development from the first electronic computer just after the Second World War to the minicomputers and microprocessors of today. Computer applications have followed the same path of development. Today, society and the individual are so dependent on these machines that society would stop functioning if they were suddenly to disappear. Their applications have resulted, by and large, in a simpler and easier existence. As with so many other technological advances, it took some time before these machines were used for activities harmful to society. One must get used to a new development before one learns to misuse it. This is also true of misuses comprising criminal offenses.

Abroad, it was not until the end of the 1950s and the beginning of the 1960s that anyone was seriously aware of the fact that a computer could be used to commit punishable offenses. The computer became a tool—a means of committing crime. Computer-assisted crime did not appear in Scandinavia before 1970, and then only in isolated instances. Throughout the 1970s authorities were aware of the existence of the problem, but those in Scandinavia were not ex-

[*] Candidate of law, Oslo University. Mr. Schjølberg served a term as a deputy judge before becoming a police attorney. He is currently assistant Chief of Police in Oslo. Since 1978 he has been associated with the Norwegian Research Center for Computers and Law in a project on computer crime under a grant from Norwegian Ministry of Justice. His report was presented to the Ministry on April 1, 1980. In December 1979 he gave a presentation on computer frauds at the 3rd Interpol Symposium on International Frauds in Paris.

posed to any sort of explosive growth in the number of such cases. This may have been due to the fact that such crimes were not being discovered, but it is more likely that the authorities were in the fortunate situation of learning from the experience of others, so that they could restrain the development of such crimes through the use of good, preventive safeguards of various types. But regardless of the safeguards employed, it is never possible to prevent all crime. Despite the enormous efforts made by American society and computer vendors, some experts estimate that the scope of computer-assisted crime[1] in the United States is at least 5 billion kroner [Norwegian crowns] annually.

One can imagine punishable offenses in many areas of the penal code which can be computer-assisted; but it is in the area of economic crime that there is the greatest experience. This article will describe instances of computer-assisted crime in Scandinavia. It is drawn from a report that is the result of cooperation between police and university authorities in the Scandinavian capitals.[2] The article is divided into eight sections. The first six group various reported computer-assisted criminal cases by the location in the computer system where the breach occurred. Section VII discussed the effect that computers are having on the penal system, while the last section suggests steps that need to be taken to cope with the inevitable increase in this form of criminal conduct.

## I. Transmission of Data from Voucher to Input

Ordinary vouchers, such as checks, notes, and invoices are being processed in a new way due to the conversion of accounts from manual systems to electronic data processing. Embezzlement and fraud will continue as before. But because data processing is being introduced, a new dimension is added to criminality. The conversion to data processing may lead to alienation, because the data contained in the system is no longer related to the individual, once it has gone into the computer. People rely on others to carry out the checking function; thus, they lack a broad overview of other figures

[1] The use of the designation "computer-assisted crime" does not exclude other relationships between data processing and crime. In the United States, the term "computer-related crime" is most commonly used, but all relationships between data processing and crime are of interest. It is undesirable to use a definition as the starting point in a field that is undergoing such constant development.

[2] This cooperation led to a seminar in Stockholm, Copenhagen and Oslo in September 1977. The American expert, Donn B. Parker, was invited to speak at this seminar, which was arranged by the Norwegian firm, O.A. Consulting. The report is part of a research project in cooperation with the Norwegian Center for Computers and Law, University of Oslo.

and relationships. The old adage "out of sight, out of mind" applies here.

This may have been one of the reasons why an employee in a bank in Norway committed gross fraud over a ten-year period, to the total of 1.4 million kroner. He developed a system using "check cavalry"[3] between a number of accounts in his own and other banks. By various accounting operations made possible by data processing he managed to keep his fraud concealed for a decade.

Completely fictitious or counterfeit vouchers can be made for computerized bookkeeping. This was the case in Sweden, where an employee of a firm falsified vouchers for entry in the computer from 1971 to 1976; in this manner he managed to get paid extra wages and vacation pay totaling 52,670 Swedish crowns (Sw.kr.). In another case from Sweden, an employee in a bank in 1976 managed to transfer Sw.kr. 5,825 from the bank's accounts to his own accounts by making false data processing entries.

From 1974 to 1975, an employee swindled the Danish postal service out of D.kr. 150,000. He made counterfeit postal giro account payment cards and applied a false stamp for debiting in the bookkeeping department from a fictitious sender and fictitious giro account number. The sums were then credited to his own giro account. He was discovered by chance when a colleague noticed the large amounts in his account. While the deficit would have shown up in the accounts of the postal giro office, it would have "drown" in the turnover of billions of kroners.

Systems can be developed that have fictitious accounts, persons, objects, and the like. This can be more easily accomplished by means of a data processing entry because continuous human evaluation and checking are lacking. The system accepts fictitious persons and information, and there is no post-evaluation of the data once it has entered the system. A street number, street name, and the name of a firm or individual that does not exist is easier to "hide" in an electronic data processing system. The risk of being exposed to a criminal violation of this kind is increased by a lack of understanding of the risks to which data processing operations are exposed, and the lack of ability to familiarize oneself with the computer's systems.

For example, in 1976 in Sweden, a person established a number of fictitious accounts without bankbooks, and then made withdrawals of S.kr. 427,500 by means of false identification papers. In 1972, an employee of a shipping company in Denmark defrauded his firm of approximately D.kr. 180,000 by creating fictitious actions for dam-

[3] This scheme is also known as "check kiting."

ages against various ships owned by the company. The payment of damages was made via data processing entries with punched cards. Pertinent information, such as ships and routes, was coded into the punched cards. The damage sums went into dummy accounts that he had established. He was discovered by accident because he coded a shipping route incorrectly.

In 1974, a young female department head in a private, Norwegian loan institution was convicted of gross fraud of almost one million N.kr. and sentenced to prison for two and one-half years. She had been a trusted employee in the firm for a long time. Her area of responsibility was document processing of installment contracts from firms with which the loan institution had discounting contracts. By setting up fictitious firms and purchasers with installment contracts, she tricked other employees in the loan institution into issuing credit notes and checks. She then shredded the credit documents for the fictitious firms and replaced them with new letters of remittance to the loan institution's bank, so that the entire amount was credited to her own savings account. All transactions were carried out by manipulating the punched cards for data entry.

To maintain the balances that the "firms" were supposed to have involved a lot of work on her part, since the loan institution's automatic, computerized reminder notice routine required that she always be up-to-date on her fictitious contracts. This she did by making out new punched cards and transferring "balances" forward in time and to new debtors. One of the reasons that she managed to carry out her activities for so long was that the bank did not send a confirmation of every transfer back to the payor. She therefore ran no risk that the firm's management or anyone else would obtain information on her transactions. The court emphasized that the situation had to be regarded as a continuous punishable offense that had extended over almost four years and was particularly serious. The court also stated that it was a matter of quite a considerable sum which she cynically and systematically, and in a particularly cunning manner, had appropriated, thus grossly exploiting her position and the trust that she was afforded by the management of the loan institution.

In July 1977, a man in Norway was sentenced to two years and six months for gross fraud of approximately N.kr. 500,000. Over a period of three and one-half years he had managed to establish thirty-five fictitious payroll accounts in a bank where he was employed. He gave one of the free account numbers available to the branch to each of the accounts he set up. Then he gave himself a checkbook imprinted with the individual account number. He put cash into the accounts by granting the fictitious persons a payroll account loan.

For making later withdrawals he first wrote a check on his own personal account in the bank, gave it to the cashier, and received the sum involved. After the check was processed by the branch bookkeeping department, he took his own check out of the bank and exchanged it for a check drawn on one of the fictitious account, which he signed and stamped. One of his jobs in the branch was to process the reminder notices which came from the data processing center. He removed and destroyed the reminder notices concerning his own fictitious accounts. This continued for three and one-half years, during which time he "dressed up" the balance amounts now and then by extending additional payroll account loans. The account statements for the fictitious accounts were removed and destroyed.

There was an audit at the branch four times a year, when the lists of overdrawn accounts were examined. To avoid being discovered, he either removed the list with the fictitious accounts while the audit was in progress, or crossed out the lines on the list where the accounts were located. If questioned by the auditors on these changes, he simply explained that the customer had deposited a sufficient amount to put the account in balance after the list had been printed. While the accused's own checkbook was taken away from him by his employer in June 1976 because of overdrafts, he still had the opportunity to take checkbooks into the bank, stamp them with his own account number, and use the checks.

In its decision, the court laid special weight on the considerable sum involved, as well as the fact that the situation continued for three and one-half years. Furthermore, he had abused his position in the bank and his detailed knowledge of routines dealing with data processing. The court also noted that by converting to EDP the bank had made the accused's activities possible. For this reason, the court found that it was important to react strongly for general preventive reasons. The court pointed out that "EDP-assisted crimes" had become a significant problem in many countries. In addition, the court emphasized that the accused acted in a systematic and premeditated manner. In conclusion, the court noted that it would not omit pointing out that the bank's conversion to data processing, which meant more efficiency for the bank, also involved a reduction in control.

The payment of wages, pensions, and the like is particularly susceptible to computer crime. Persons who are not entitled to payments, because they are sick, left the firm, are on vacation, or have died, can be kept in the system for varying lengths of time. Time card information from other employees can also be abused. Monthly totals and annual totals are figures that can be the object of manipulation. Rounded-off figures in tax calculations or percent calculations are also tempting targets. The individual wage-earner often does not have the time or the ability to check these totals. Special checking of employees and special key persons are important safeguards in this area. In addition, there must be an evaluation of the number of persons and their different functions.

Programmers should not also be computer operators, nor should the latter have access to the basic programming documents. In March 1977, a Norwegian woman was sentenced to prison for two years for gross fraud against the firm where she was employed. Over a period of almost one year, she had defrauded the firm of approximately N.kr. 350,000. The payroll system in the firm was computerized. After a short training period, the woman was given the responsibility to calculate wages for data processing entry and, when the wages had been calculated by the computer, to make cash payments of the wages to employees. After some time, this became too tempting for the woman and she began to enter names on the payroll list of persons who were not entitled to wages. This was done, in particular, for those who were out due to sickness, were on vacation, or had left the firm. She calculated the gross amount as if they were still working, and deducted the taxes that were to be paid to the tax authorities. She placed the net wages in a payroll envelope after calculation by the computer, but took the envelopes herself.

Complaints started coming from workers about incorrect hourly wages and incorrect income entered on the wage statements. The complaints got no further than the woman, who dismissed them as nonsense. The management of the firm was finally informed. It took a long time for the situation to be discovered, and it was purely by chance. One of her colleagues found some empty payroll envelopes with names on them in a wastebasket in the woman's office—envelopes into which she had helped put money. At about the same time, the colleague discovered that two wage statements that the woman handled, which should have had sixty-eight hours entered on them, had been credited with eighty-five hours. The woman had tricked the cashier into paying out cash, which was put into payroll envelopes, on the basis of falsified payroll account entries. No receipt was given for these envelopes.

The court stated that it could not overlook the fact that the firm's arrangement for the payment of wages made it relatively easy for the defendant to unlawfully divert funds to herself in the way she did. The court described her method as bold and skillful, and held that out of concern for general law-abiding behavior a firm reaction was required.

## II. Input

Payment and disbursement cards, cash cards in the Postal Savings Bank and the like, are pre-punched cards. With a manual punching machine, it is possible to make additional holes in the card. Other holes can be filled. This type of action should be caught by forwarding agents and receivers; if it not caught the computer will generally reject the punched card. If, however, acceptance takes place locally and the data is processed centrally, the perpetrator will gain time. As an example, in two cases from Sweden in 1972, a person made extra holes on a telephone bill that was a punched card, so that subsequent input of the card to the computer system showed that he paid S.kr. 1,000 extra in each instance than he actually had paid. The excess amount was credited to his account.

A data processing consultant employed by a Danish computer firm in 1968 falsified payment cards to an oil company with a manual punching machine by adding new holes and covering old ones. The machine-written amount on the payment card was paid at the post office, while the excess amount punched falsely on the card was credited to his account at the oil company.

The automat system consists of a card, most often of plastic, bearing the account number and other pertinent information, and a number remembered by each person which is keyed at the same time the card is inserted in an automat for money, goods or other services. While the gain may be a limited amount, it is possible to transfer money from one account to another in this manner. In addition, these transfers may be done by telephone with special additional equipment for insertion of cards and information. The system is in its infancy in Norway, but in other countries there have been major problems with punishable offenses committed using these machines.

In Sweden, a perpetrator in 1976 diverted S.kr. 872,928 to himself by establishing fictitious personal accounts, counterfeiting "bancomat cards," and making withdrawals from bank automats on a grand scale.

## III. Programming

Via programming, the computer can be given instructions for unauthorized problem solutions. This is a more advanced type of computer crime, which requires technical knowledge of the computer and its method of operation. The perpetrator makes use of the computer in an unauthorized manner. Large-scale programs may be used to carry out a criminal offense.

An example from Norway involved the Postal Savings Bank's payroll account system. This system is based on the use of "cash cards," which are pre-printed and pre-punched cards on which the amount to be taken from the account is manually entered. Each account has its own special mark in punch holes and printing. On June 25, 1976, cash cards were presented for payment for a total of N.kr. 5,000 at three different post offices in Oslo. The postal clerks paid out the amounts and noted the identification that was shown. When the cash cards went into the data processing center, they were rejected as invalid. The names and birthdates used on the three cash cards were of non-existent persons. The cash forms was the same, and it was ascertained that they were from a printing in January 1974. In the Postal Savings Bank's own warehouse there were only cash cards from the 1976 printing.

Upon close inspection of the counterfeit cash cards, a false transaction type was found, as well as the fact that all three cards were numbered with the number "8". These facts indicated that it was not the correct program for the Postal Savings Bank that was used. It was, therefore, suspected that a new program had been written for these spurious cards. To accomplish this, the perpetrator would have needed knowledge of how the computers were run, knowledge of programming, and access to a computer center where this program development could be performed. Therefore, it was decided to carry out a test run at all computer centers in Oslo that had this special printing and punching unit. Because the investigators had certain clues due to the special mark in the printing of the counterfeit cash cards, and because the postal clerks were able to provide a good description of the person involved, the perpetrator was caught.

He had a background both as a computer operator and programmer, and had worked in 1974 for a firm which had a contract with the Postal Savings Bank. At that time, he took home a stack of fifty cash card forms. After studying a pre-punched and printed cash card, he was able to counterfeit false cash cards. He invented the necessary information and constructed a fictitious person. By using the computer at the firm at which he was then employed, he was able to run the cash cards. For this purpose he availed himself of a large program supplied by the vendor of the computer. Altogether he produced almost fifty cash cards. He had no previous criminal record and was sentenced to prison for six months, of which twenty-one days were with no opportunity for parole. The court made special mention of the general preventive aspects, and that the accused had used his position as a programmer in a data processing center to produce counterfeit cash cards.

Another possible abuse is where a program is entirely or partially stolen or removed. The results of such acts will be that problem solutions are completely incorrect or not given at all. Punishable situations will be the same as in ordinary thefts and embezzlement.

Additions can also be made to existing programs, or false information input, which, in turn causes improper responses from the computer. Two cases from Sweden should be mentioned in this connection. In one of them, an employee set himself up as a payment recipient in the employer's computer center in 1975, and diverted S.kr. 37,892 to himself in this manner. In the second case, in 1973, the central Swedish automobile register was fed false information.

Alterations in existing programs may consist either of something active being carried out, such as instructions for the transfer of funds from one account to another, or something more passive, such as bypassing automatic reporting routines when carrying out misuse of an account. In an example from Sweden, during the period 1960-1966, a bank employee transferred S.kr. 122,975 from a bank account with low activity to his own account. In another example from Sweden, in 1974, a person made false punched cards which caused unauthorized payment of S.kr. 263,669 to be made to his bank giro account from his previous employer.

In a case from Denmark, an employee in a bank diverted D.kr. 120,000 to himself over a period of several years by setting up a fictitious cash credit account in the name of an existing person. In order to prevent the bank balance statements from being sent to the addressee, he programmed the machines to ignore the usual procedure in this case. If the balance in the cash credit account exceeded the maximum credit line, due to finance charges and debiting of bank fees, he programmed the computer so that each debit transaction of this type automatically raised the maximum credit line accordingly. He was discovered two years later because of thefts from the bank. At that time, he had closed the cash credit account by transfers from the bank's collective account for finance charges and fee income—a transfer which also was not discovered for two years.

## IV. Computer Hardware

Punishable actions may also be aimed directly at the destruction of or damage to vital hardware units. There have been some cases of this type in Scandinavia. In 1972, an unknown person cut off the power to the computer center for Bromma airport in Sweden, and the same year all of IBM's offices in Sweden were subjected to bomb threats by unknown persons.

Damage to a computer center has also occurred in Sweden. On

June 11, 1973, a person stole a "circuit board" from a computer. The value of the board was estimated at S.kr. 96,000.

## V. Data Transfer

Actions in this case may consist of copying programs, data, and the like which firms, public institutions and others have set up, or to search for information from the registers to aid in carrying out the wrongdoing.

In Sweden, a person in 1970 copied the address lists from his previous employer's computer center when he started his own company. The list was valued at S.kr. 100,000. In addition, in 1974, unauthorized copying of computer data was carried out in Sweden.

In Norway, in 1972 a person employed in a government loan institution was sentenced to prison for one year and two months for gross fraud and forgery. He was the leader of the loan institution's data processing operations group and, in the course of three days, he tricked the Post Office into paying him a total of N.kr. 155,000 on false instruments of debt. In the loan institution's computer center, he selected a name of an existing person at random with running number, code and other necessary data. He then filled out forty-six identical instruments of debt with the same name, of which he used twenty-five.

The punishable offense may also consist of copying checks, payment cards, cash cards, and the like, which are printed or issued directly by the computer. There is evidence of at least one such instance from Sweden, where a person in 1974 made eighty-six false payroll payment cards for himself on his employer's computer and obtained a total of S.kr. 262,710 by using them.

## VI. External Data Communication

In the case of external data communications, punishable offenses may consist of tapping telephone lines, satellites, or the like by electronic means. Though there are no known cases which have occurred in Scandinavia, there is one from England. A fifteen-year old schoolboy completely destroyed the system in a computer service office in London. He managed to obtain access to top secret files which other users had in the computer, and could read and alter them as he wished without notice. He used no special technical devices, and started without any specialized knowledge of the internal operation of the computer, but relied instead upon himself and a computer terminal at his school. The boy listened to the communications of authorized users with the computer in order to pass himself off as one of them and obtain access to the files. He succeeded in taking over the system completely, cutting off other users, changing passwords, and even changing invoices which customers were to pay.

## VII. Effects of Computers upon the Criminal Penal System

Technological developments must be compared to existing regulations in the penal code and the criminal trial law to determine whether the regulations are sufficient. Will the development of data communications have any effects on the criminal penal system, and if so, what will be those effects?

The cases assumed to be computer-assisted which have been tried in Norway have not caused any problems. The regulation in the penal code regarding fraud has been used, and the courts have approved of it. But the Norwegian cases are not very technologically advanced, and the Danish and Swedish examples show the problems involved.

Will authorized external access to the computer installation, for example, via punched-card reader or on-line terminal, be considered burglary, and be punishable under § 147 of the Penal Code,[4] or can § 145[5] or § 145(a)[6] be used? How is data communication related to

[4] Section 147 provides:

Anybody who unlawfully breaks into or assists another in breaking into a house, vessel, railroad car, automobile or aircraft or into any room in same or into a closed courtyard or similar storeroom or place of residence, by damaging an object designed for protection against intruders, or by means of a picklock, false key or key unlawfully taken from the possessor, is considered guilty of punishable burglary.

Anybody who is guilty of burglary or is accessory thereto, shall be punished by imprisonment up to one year. If the felony is committed by an armed person, or by several in cooperation, imprisonment up to two years may be imposed; if the felony is committed with the intent to prepare the way for another felony, imprisonment up to four years may be imposed.

Anybody who by violent or threatening conduct seeks to force his own or another's unlawful admission to, or presence in, such place, or who unlawfully sneaks into an inhabited house or room which usually is kept closed at night, with the intention of being locked in, or who by means of disguise or pretended or misused public capacity or order, or by use of a document which is falsified or pertains to somebody else, obtains for himself or another, unlawful admission to or presence in an inhabited house or room, or is accessory thereto, shall be punished similarly.

Penal Code § 147.

[5] Whoever unauthorized breaks upon a letter or other closed document, or breaks into another's 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, etc.

If injury is caused through knowledge acquired thereby, or the felony is committed for the purpose of unlawful gain, imprisonment for up to two the legal definition in § 6 of the Penal Code[7]? Will programs or data in the data processing installation be considered movable articles, objects, or subject to property law? The relationship to § 255 and § 257 of the Penal Code,[8] in other words, may be a central problem. In conjunction with embezzlement, the question also arises of whether the perpetrator had "movable articles" in his possession when, for instance, he alters a program so that all increases from 0.5 to 0.9 are transferred to a special account.

Are the regulations of the criminal trial code concerning search and seizure sufficient when computer equipment is to be evidence? Spools of magnetic tape contain colossal amounts of information, and the evidence required probably is located on only part of the tape. Should special procedures be developed instead of impounding all tape reels? The consequences could be quite serious for firms which have all of their accounts, customer files, and the like in the computer system, and are dependent upon the continued availability of these files and data. These difficulties will be important for the procedure used in the confiscation of evidence. There is also the question of the procedure to be used in scrutinizing evidence and in the depositions of any experts.

> years may be imposed. Public prosecution may not be initiated without the request of the victim.

PENAL CODE § 145.

[6] Section 145(a) provides:

> Fines or imprisonment up to six months may be imposed on anybody who
>
> 1. with the aid of a concealed monitoring apparatus, listens to a telephone conversation or other conversation between other people or to negotiations in a closed meeting in which he himself does not participate.

[7] Section 6 of the Penal Code provides "[t]he term movable object as used in this code includes any power made or stored for the production of light, heat or motion."

[8] Anybody who, for the purpose of obtaining an unlawful gain for himself or another, illegally disposes of, pawns, consumes or otherwise appropriates any movable object which he has in his custody but which totally or partially belongs to another, or unlawfully disposes of money which he has collected for another or which is entrusted to him, may be punished for embezzlement.

> Punishment according to this section shall not apply to acts punishable under sections 277 and 278.
>
> The punishment for embezzlement is imprisonment up to three years. Complicity is punished in the same way. Under extreme extenuating circumstances, fines may be imposed.

PENAL CODE § 255.

> Anybody who carries away, or is accessory to carrying away, an object which totally or partially belongs to another, for the purpose of obtaining by the appropriation of such object an unlawful gain for himself or another, shall be punished for larceny.
>
> The punishment for larceny is imprisonment up to three years.

*Id.* § 257.

How should investigators, auditors and experts be trained to provide the best possible assistance in the criminal trial system? This question, along with the very important problem of what preventive measures should be implemented, will naturally demand that a solution be found.

## VIII. Conclusion

In order to understand these problems and the effects that they will have on the Norwegian criminal trial system, it is necessary to gather and analyze more material than we have today. The country which has the most experience with this type of crime is the United States. On the basis of the greatest possible number of examples from there and from other countries, we will obtain the best foundation for evaluating the significance for Norway and the other Scandinavian countries.