Marmara İletişim Dergisi, Sayı:6, Nisan 1994

SEMANTICS OF COMPUTER CRIME IN THE EC

Rauf H. ÖZARSLAN
Research Assistant
MARMARA UNIVERSITY
Faculty of Communications

CHAPTER 1: INTRODUCTION

Computer crime' is a rather diffuse topic and it is hard to agree upon definitions. It is not, of course, a precise legal category. Theft or deception offenses, for instance, may be committed with or without the use of a computer, and it is rare to find offenses which are applicable solely in a computer environment. Computer crime is an artificial overlapping class of lawbreaking which is uncertain in scope. Some definitions insist that the category of computer crime must involve the highly skilled operation of a computer in circumstances where the offence could not otherwise have been committed.

Extreme legislative responses have led some sceptics to the opposite extreme view that computer crime is a complete myth, in the sense that it merely represents new ways of committing old offenses, and that existing criminal laws are more than capable of dealing with it. A corollary of the latter view is that there is `nothing special' about computers, and that it would be anomalous to create specific criminal law provisions to take account of them. This is simplistic, and a mistake (WASIK 1991). It is suggested, however, that the sheer diversity of behaviour within the context of computer misuse, where the computer may figure at one moment as the instrument of crime, and at the next as the target for crime, and given the apparent importance of non-economic motives in some forms of computer misuse, such as the unauthorized access of computer systems purely for intellectual challenge and some cases of computer sabotage, makes any monolithic explanation of this phenomenon quite impossible.

Numerous different categorizations of computer misuse have been designed by different writers for their particular purposes, influenced by whether the issue is being addressed primarily in terms of describing the practical impact of the most prevalent varieties of misuse, or in terms of identifying the specific legal issues. Cornwall(1987) writing for a non-specialist audience, uses the broad non-technical categories `Datafraud', `Dataspying', and `Datatheft'. Sieber(1986), however, a German legal expert, adopts a more comprehensive sixfold classification: (a) fraud by computer manipulation , (b) computer espionage and software theft, (c) computer sabotage, (d) theft of services, (e) unauthorized access to data processing systems, and (f) traditional business offenses assisted by data processing.

In this study, I will try to demonstrate the dimensions of the problem of computer crime from various aspects; especially the issue of computer fraud and other elements that constitute computer crime. In the flow of this study I will investigate the Legislations of some European countrries for tackling the problem, especially the `Data Protection Acts' and `Computer Misuse Act in Britain'. Giving a clear definition of these acts will give us the foundation to understand the semantics lying behind and therefore help us achieve the main aim of this study, `What constitutes computer crime'.

At the conclusion, I would like to apply the semiotic framework as an approach to demonstrate the boundary of computer crime as a system.

CHAPTER 2: ANALYSIS OF DATA PROTECTION ACTS OF UNITED KINGDOM, GERMANY AND FRANCE

DATA PROTECTION ACT 1984 UK:

- Purpose and application of the act:
  . Purpose:

To regulate the use of automatically processed information relating to individuals and the provision of services in respect of this information.

In practical terms this means that when use is made of automatically processed personal data or when services relating to personal data are employed the DPA will protect the individual against:

(a) the use of personal data that are inaccurate, incomplete or not relevant.

(b) the possibility of unauthorized access to, or examination of the data; and

(c) the use of data for a purpose other than that for which it was ori ginally collected.

SUBJECTS

The DPA is aimed at the following subjects:

(a) the data subject;

(b) the data user;

(c) the computer bureau

Data subject: Every living individual member of the population is potentially a data subject: "an individual who is the subject of personal data"

Data user: `Data user' means a person who holds data, and a person holds data if-

(a) the data form part of a collection of data processed by or on be half of that person; and

(b) that person(either alone or jointly or in common with other per sons) controls the contents and use of the data comprised in the collection; and

(c) the data are in the form in which they have been or are intended to be processed as mentioned in paragraph(a) above or (though not for the time being in that form) in a form into which they have been con verted after being so processed and with a view to being further so pro cessed on a subsequent occasion.

Computer Bureau: A person carries on a `computer bureau' if he provides other persons with services in respect of data, and a person provides such services if -

(a) as agent for other persons he causes data held by them to be proces-

sed; or

(b) he allows other persons the use of equipment in his possession of data held by them.

OBJECT: Processing of personal data

Processing: Processing, in relation to data, means amending, augmenting, deleting or re-arranging the data or extracting the information constituting the data. In the case of personal data, it means performing any of the above operations by reference to the data subject.

Personal data: Data are defined as "information recorded in a form in which it can be processed by equipment operating automatically in response to instructions given for that purpose."

Personal data are defined as: "data consisting of information which relates to a living individual who can be identified from that information(or from that and other information in the possession of the data user), including any expression of opinion about the individual but not any indication of the intentions of the data user in respect of that individual."

The DPA draws a distinction between three types of personal data:

(a) factual personal data - this category comprises data that present facts. Examples are: name, address, membership of trades union, ma rital status, age, family members, results of psychological tests, re sults within the company, etc.;

(b) value judgements - this category comprises subjective opinions and views about an individual. Here one can reckon a person's credit worthiness, promotion prospects, etc. The views of third parties, for example testimonials supplied by referees of the applicant, may be brought under this category;

(c) intentions - this third category comprises data that express the in tentions of the data user towards the data subject. Career paths are a good example.
Exemptions:

Apart from data that by definition cannot be characterized as personal

data there are data that are undoubtedly personal data but nevertheless fall partly or entirely outside the act. The DPA draws a fourfold distinction between:

(a) personal data that are entirely exempted form the operation of the Act;

(b) personal data to which the provisions relating to third-party disclo sure do not apply;

(c) personal data that are excluded from the right of access;

(d) personal data in regard of which the right of access can be modified.

Please See Appendix A for a detailed explanation of each of the above exemptions.

RIGHTS AND OBLIGATIONS:

The rights and obligations pertaining to the private sector may be divided into four categories, namely;

(1) the Eight Data Protection Principles(hereafter,the DP principles)

(2) the obligation to register in the Data Protection Register (hereafter, the Register)

(3) the obligation to permit access by data subjects

(4) the exemptions

Please See Appendix B for a detailed explanation of rights and obligations.

TRADING PERSONAL DATA:

The DPA provides two exceptions of importance to the trade in personal data. First, there is a partial exemption from the operation of the DPA for personal data held for statistical and research purposes. Secondly, personal data held by credit-reference agencies are in part relieved of the obligations under the DPA.

OBLIGATIONS OF THE COMPUTER BUREAU:

The obligations of a computer bureau are more limited than those of a data user. Compliance with the Eighth DP principle, with the duty to register, with a disclosure prohibition and with a prohibition to depart from the data user's register entry, is required.

(a) Obligation to register: Computer bureaus are subject to a reduced registration duty under section 4(4) DPA: the entry shall consist of the name and address of the computer bureau. It is unnecessary to register other matters.

(b) Disclosure prohibition: The computer bureau may not knowingly or recklessly disclose the personal data without the authority of the da ta user for whom the services are provided unless one of the non-disc losure exemptions applies. Doing so constitutes a criminal offence.

GERMAN DATA PROTECTION ACT:

ANALYSIS OF THE BDSG (Act on Protection against the Misuse of Personal Data in Data Processing in Germany):

- Purpose of the Act: The purpose of Data protection is to ensure aga inst the misuse of personal data during storage, communication, mo dification and erasure (data processing) and thereby to prevent harm to any personal interests of the person concerned that warrant protection.

SUBJECTS:

The BDSG distinguishes between three subjects, namely, (1) the data subject, (2) the data user and, (3) the computer bureau.

- Data Subject: Only a natural person can be a data subject. A supple mentary condition is that the person must be living in order to enjoy the protection of the BDSG.

- Data User: Controller of the file shall mean any of the persons or bo dies (physical or legal persons, companies or other private-law associ ations), which stores data on its own account or has data stored by ot hers.

The BDSG divides data users of personal data into two categories, to which different rules apply:

(a) data users which process personal data for their own purposes.

(b) data users where the prior objective of processing personal data is to disclose the same commercially to third parties. (Commercial pro cessing of personal data by private enterprises such as credit rating agencies, data banks, market research agencies, and the like).

- Computer bureau: The BDSG provides no further definition of computer bureau. The reference is normally to the person who by order of the data user processes data.

OBJECT: The processing of personal data

What is the object of the BDSG? The object of the BDSG is the processing of personal data. Please refer to appendix C for a detailed explanation of processing and personal data.

RIGHTS AND OBLIGATIONS:

Rights of the data subject: In principle every data subject has the right to;

1. Information on stored data concerning him: The data subject has a right to information concerning stored data relating to him. If the data are processed by computer the data subject also has the right to be informed as to which persons and organizations these data are regularly disclosed.

2. Correction of any incorrect stored data concerning him: Personal data must be corrected if inaccurate.

3. Blocking of stored data concerning him where their accuracy or inaccuracy cannot be established or where the original requirements for their storage no longer apply: Personal data must be blocked when their accuracy is challenged by the data subject and the accuracy or inaccuracy cannot be determined. Blocked data may not be processed or used.

4. Erasure of stored data concerning him where such storage was inadmissible or - as an option to the right of blocking of data - where the original

requirements for storage no longer apply: The destruction of personal data is permitted when it may be presumed that the interests of the individual would not thereby be prejudiced.

Obligations of the data user:

(a) when is processing permitted? The processing of personal data is permitted when:

- The BDSG or another legal provision so permits, or

- The individual concerned has given permission for data relating to him to be processed.

(b) relationship with the purpose: Those involved in processing are not permitted, without authorization, to "process, communicate (to third parties), grant access to or otherwise use protected personal data for any purpose other than that of the legitimate accomplishment of their task."

(c) security obligation: There is an obligation on all persons involved in processing data within the scope of the BDSG to implement techni cal and organizational measures to ensure that the act is complied with.

Obligations of the computer bureau:

(a) relationship with the purpose: The obligation imposed on data users only to process, disclose, grant access to or otherwise to use per sonal data in accordance with the purpose for which they were stored applies mutatis mutandis to computer bureaus.

(b) security obligation: The obligation to take security measures app lies in equal measure to computer bureaus.

(c) obligation `to keep to the contract': The computer bureau may pro cess the personal data only within the terms of the contract and follo

wing the instructions of the data user.

FRENCH DATA PROTECTION ACT - Loi relative a l'informatique, aux fichiers et aux libertes (hereafter, LIFL):

- Purpose of the act:"Data processing shall be at the service of every citizen. It shall develop in the context of international co-operation. It shall infringe neither human identity, nor the rights of man, nor privacy, nor individual or public liberties."

This description of the purpose of the act is broader than that of the German and English legislation on privacy which are confined to just one aspect of information technology, namely, the processing and use of stored personal data whether in automated or non-automated systems. The choice was made not to restrict the French legislation in that way. The LIFL is principally directed at regulating the processing and use of automated and non-automated personal data.

SUBJECTS:

(a) Data subject: No definition of the concept of data subject is provi ded by the LIFL. It can be deduced from the act that every living per son whose personal data are subjected to automated or non-automated processing qualifies as a data subject.

(b) Data user: Nor is the concept of data user defined in the LIFL. It may be deduced from the act that a data user is the person who decides whether personal data are to be processed, by computer or otherwise. A data user may be either a natural person or a legal entity.

(c) Computer bureau: The computer bureau is not addressed by the LIFL.

OBJECT: the processing of personal data:

In general terms the object of LIFL is data processing, data files and individual liberties. The object may be defined more specifically as the automated, non-automated and mechanized processing of personal data.

Processing: "For the purposes of this act the automatic processing of

personal data means any series of operations effected by automatic means, involving the collection, recording, preparation, modification, storage and destruction of personal data as well as any series of such operations relating to the use of files or data bases, including interconnections or comparisons, the consultation or communication of personal data."

Automated processing is thus regarded as encompassing everything involving the collection, recording, processing, amending, storing and destruction of personal data relating to an automated process as well as all those factors in relation to the utilization of a file or a data bank. The act expressly and emphatically points out the fact that the acts of linking or comparing, of unilaterally consulting or interactively communicating are also to be understood as falling under automated processing. Non-automated processing is not further defined. Mutatis mutandis, the same description must be applicable. That also applies to machine processing.

Personal data: Personal data are data which permit, in any form, directly or indirectly, the identification of the natural persons to which they relate.

Exemptions: Only in one instance are personal data excluded entirely from the operation of the LIFL and that is where non-automated and mechanized processed personal data are intended exclusively for personal use, for example, addresses entered into a diary.

Partially exempted: (a) non-automated and mechanized processed personal data not intended exclusively for personal use and (b) most common types of private processing of automated personal data which manifestly do not infringe privacy or liberties.

RIGHTS AND OBLIGATIONS:

Rights of the data subject:

(a) Right to know: Every data subject has the right to know that data relating to him have been entered in a file, who the data user of the file is, where that file is located and for what purpose the entry was made.

(b) Right to object: Section 26 LIFL gives every data subject the right to refuse the processing of personal data relating to him. The refusal must be founded on legitimate reasons. What one is to understand by

this is not regulated in the act but must be determined on a case-by-case basis.

(c) Right to access: Section 34 LIFL gives every data subject a right of access of the personal data relating to him:"Any person providing his identity shall be entitled to question the departments or organizations using automatic processing, to determine whether such processing involves personal data concerning him, and if they do, to obtain access thereto."

(d) Right to correction: If personal data are inaccurate, incomplete, ambiguous or out of date, or if collection, use, disclosure to third parties or storage are prohibited, the data subject may have the data amended, supplemented, clarified, brought up-to-date or destroyed.

An important question here is with whom the burden of proof lies that the data are inaccurate, incomplete and so on. The solution that has been chosen is this: if the data were supplied by the data subject himself or if he agreed to their processing the burden of proof rests with him. In all other cases the burden of proof rests with the data user.

Obligations of the data user: General obligations: Of the general obligations for the data user to be discussed in this section, those at (a), (b) and (g) concern automated as well as non-automated and mechanized processed personal data while the obligations at (c), (d), (e) and (f) apply only to automated personal data. Please see Appendix D for a detailed explanation of obligations.

Obligations of the computer bureau: Nowhere does the LIFL refer to the services provided by computer bureaus. The Act is concerned exclusively with the data user and the data subject. Accordingly, within the terms of the French law on privacy, the data user is always to be seen as the person responsible for the processing of personal data in conformity with the requirements imposed by law. Furthermore, he is the one who has the power of decision in respect of the processing to be carried out; a computer bureau, in contrast, acts only on his order.

CHAPTER 3: SEMANTICS OF COMPUTER CRIME

Unauthorized Access and Unauthorized Use: In those jurisdictions where there has been the greatest development of the criminal law in response

to computer misuse, particularly the United States, the most important approach has been to criminalize the initial unauthorized access of the computer. The American approach has been followed in several other jurisdictions, and it has been adopted in Britain, with the passing of Computer Misuse Act 1990. While there is much to recommend this strategy, and it seems the best approach overall, objection may be levelled at criminalizing and recommending a heavy punishment for what is essentially a preliminary act of `tresspass'. Tresspass into someone's home is ordinarily a civil rather than a criminal wrong and it seems anomalous that tresspass should amount to a criminal offence merely because a computer is involved. The English law commission produced a report proposing the creation of a basic offence of `unauthorized access to a computer', punishable in a magistrates' court, and an `ulterior intent' offence, where the unauthorized access was accompanied by an intent to commit or facilitate the commission of a serious crime (Wasik 1991).

Hacking: If we envisage a person such as a hacker, working entirely from motives of curiosity, and merely inspecting data without changing anything, such accessing of the computer was not, prior to the Computer Misuse Act 1990, a criminal offence. Should it be? Some argue that `pure hacking' is harmless, indeed even socially desirable, in that it may point to up security weaknesses in computer systems which can be remedied before being exploited by less well-intentioned individuals. On the other hand, the main arguments in favour of creating a specific offence of `computer tresspass' are that, given the great and increasing importance of computers in modern society, it is in the public interest that those who use and rely upon computers should not be hampered by the fear that others may gain unauthorized access to material held on the computer, particularly where that information is sensitive or confidential.

In its report on Computer Misuse, issued in September 1989, the Law Commission recommended the creation of three new offenses, one of which was the `basic unauthorized access' or `basic hacking offence'. The offenses in the Computer Misuse Act 1990 are squarely based upon the wording in the Law Commission's Report. By section 1 of the Computer Misuse Act 1990:

(1) A person is guilty of an offence if-

(a) he causes a computer to perform any function with intent to se cure access to any program or data held in any computer;

(b) the access he intends to secure is unauthorized; and

(c) he knows at the time when he causes the computer to perform the function that that is the case.

(2) The intent a person has to have to commit an offence under this sec tion need not be directed at-

(a) any particular program or data;

(b) a program or data of any particular kind; or

(c) a program or data held in any particular computer.

By section 17(5) in the Computer Misuse Act, access is defined as `unauthorized' if the defendant is not himself entitled to control access to the program or data and he does not have the necessary consent from any person who is entitled to give it.

The term `computer' is left undefined in the Act, endorsing the Law Commission's view that it would be `unnecessary' and `foolish' to provide a definition.

The central phrase in the hacking offence is `causes a computer to perform any function'. Another way of designing a hacking offence would be to define it in terms of `unauthorized access' and then to rely on the law of attempt to cater for the unsuccessful hacker (Wasik 1991).On the other hand, the breadth of the unauthorized access offence would also cover some perhaps surprising cases, such as the employee who, knowing that he is not authorized to view particular data, switches on the computer on his desk in order to try to do just that. If intent can be proved, by switching on the machine the employee has `caused a computer to perform any function' and he would, without more, be guilty of the offence. Careless, inattentive, or even reckless accessing of computer-held material is not sufficient to establish this offence, though recklessness would have been a sufficient fault element under Miss Nicholson's Bill. Once the defendant knows he is unauthorized, he would commit the offence as soon as he `causes the computer to perform any function' with intent.

Wiretapping and Eavesdropping: In the United States , use of wire, telephone, or television communication facilities for the purpose of executing a scheme to defraud or obtain money or property by false pretences is a federal

offence even where the underlying fraudulent activity is strictly not a federal or state offence. The wiretapping laws predate and hence were not designed to deal with the problem of unauthorized access to a computer, and whether they apply in a given case is inevitably somewhat arbitrary. The English law commission stated that any new offence of obtaining unauthorized access to a computer should not extend to computer eavesdropping, because of the anomaly of creating a special offence in relation to computers where spying and surveillance generally does not come within the criminal law. The commission specifically excluded `listening in' to a computer from a distance from the scope of their proposed `basic hacking offence' and `ulterior intent offence', with the additional argument that the kind of conduct involved in electronic eavesdropping does not pose a threat to the operational integrity of the system concerned in the way that hacking does, but is aimed more specifically at the confidentiality of the information which it contains. The commission's view was, in turn, criticized as being too narrow an approach, with critics urging a definition of `access' broad enough to cater for `the emergence of this new threat'. On balance, though, it is difficult to refute the Law Commission's argument and, with one possible exception, their proposed offences, as adapted and defined in the Computer Misuse Act 1990, would seem to exclude criminal liability for computer eavesdropping. The only situation where such conduct might fall within the terms of the basic hacking offence is where the monitoring device used by the eavesdropper can itself be regarded as a `computer'. If it were to be so regarded in law, then the eavesdropper would be guilty of the basic hacking offence where he causes(his) computer to perform any function with intent `to secure access to any program or data held in (the target) computer'.

Data Protection Offences: In most countries computer-related infringements of privacy have primarily attracted the attention of the civil law, though there has been some criminal law development in protecting some rights related to privacy, such as in trade secrets and the interception of communications, or by the creation of special data protection and privacy statutes. Many European privacy laws catering for data protection, however, involve the criminal law to a much greater extent, and include comprehensive lists of criminal offences with high maximum punishments. These cover such matters as the unauthorized collection, recording, and storage of data, the unauthorized obtaining of or access to or disclosure of data, or the unauthorized use of data. In the United Kingdom, the Criminal law is not widely used in the Data Protection Act 1984 or indeed in the protection of privacy generally. The offences under the Act are `last resort' remedies, which can only be initiated by the

Data Protection Registrar, or with the consent of the Director of Public Prosecutions. Offences under the Act have already been explained in the analysis of the Data Protection Act.

Misuse of Computer Time and Facilities : A common form of computer misuse involves the accessing of a computer in order to make use of computer time or facilities to which the person making access is not entitled. This may be done either by a person who has authorization to use the computer at other times or for other purposes, or by an outsider, by hacking.

It is apparent that sometimes cases of misuse of computer time or facilities will fall within the scope of the new offences in the Computer Misuse Act 1990.

A possibility to establish liability is prosecution for theft. The English law of theft does not cover the abstracting of intangibles such as computer time and facilities. A theft charge would only be effective where tangible property was removed consequent upon the misuse of computing facility. Accepting the general inapplicability of a charge of theft to unauthorized use of computer time or facilities in England, more promising perhaps, on the face of it, is a prosecution for obtaining services by deception, under section 1 of the Theft Act 1978. It provides that:

> (1) A person who by any deception dishonestly obtains services from another shall be guilty of an offence.

(2) It is an obtaining of services where the other is induced to confer a benefit by doing some act, or causing or permitting some act to be done, on the understanding that the benefit has been or will be paid for. Several fact situations may be distinguished. First, the defendant may gain access by pretending to be an authorized user. He may have obtained an authorized user's password, or he may `piggyback' on an authorized user's line. If permission to access the system is obtained via the computer's electronic access control, then the difficulty is that no deception has operated on a human mind. This effectively rules out liability for any crime based on `deception'. Second, the defendant may be an employee of the computer owner, who normally has access to the computer but who on this occasion uses it outside working hours in order to develop or run his own programs. Again, the unauthorized access would presumably involve no deception of a human mind and so the charge would fail. The third situation is where the employee uses the computer for his own

purposes during normal working hours. There is still the problem of absence of deception and no `permission'.

One of the problems with proposals to criminalize unauthorized use of computer time and services is that the great majority of such behaviour which occurs is very trivial and hardly justifies the use of the criminal law. It is the disciplinary action taken by an employer. The question is how to distinguish these cases from the few serious cases where the defendant may be running his own profitable business in his employer's time, using his employer's computing facilities.

There seems to be nothing to distinguish the misuse of an employer's computer from the misuse of the office photocopier or typewriter, and that it is therefore inappropriate to invoke the criminal law to punish conduct more appropriately dealt with by disciplinary procedures. Again, however, the new offences proposed by the English Law Commission which, with some amendment, have been adopted in the Computer Misuse Act 1990, could on occasions extend to cases where the defendant's object was the obtaining of computer time or resources. Clearly, if an employee without permission accesses a program on his employer's computer for his own personal use, that conduct would fall within the basic hacking offence under section 1 of the Act. There might also be an offence of `unauthorized modification of computer material' committed under section 3 of the Act; the offence is where the defendant without authorization modifies material held on a computer with intent to impair the operation of the computer or to impair the reliability or accessibility of data stored there. This might sometimes cover the case of an employee running his own business on his employer's computer. Where the unauthorized use was heavy, other people seeking access to the computer might well be prejudiced, but to obtain a conviction the prosecution would have to prove that the defendant by his own access thereby intended to impair the reliability or accessibility of data for others.

Computer Fraud: The most helpful way for present purposes in which to look at computer fraud is that adopted by the Audit Commission of England and Wales:it divided this category into "input frauds", "output frauds" and "program frauds".

a) Input Frauds: This kind of fraud can be defined as dishonestly entering false data into a computer, or dishonestly suppressing or amending data as it is keyed in. The Audit Commission's survey (Survey of Computer Fraud

and Abuse) found that input fraud was by far the most common type of fraud identified by respondents, probably because it does not require a sophisticated understanding of the computer system. Some cases for input frauds are as follows:

Case 1: Amount: £20,000 Duration: 4 weeks

Perpetrator: Buyer

The Computer system was used to generate a purchase order for goods that were not required and never delivered. The buyer, in partnership with an outside agent, hoped that the company would pay the invoice. Internal checks prevented the invoice payment and investigation showed that the order had been raised without authority.

Case 2: Amount: £4,678 Duration: 6 months

Perpetrator: Clerk

The perpetrator was employed in assisting in the preparation of urgent data in respect of benefits. Whilst employed and also for a period of time following his voluntary termination of employment, the perpetrator:

(a) fraudulently made out spurious claims;

(b) forged the authorising officer's signature;

(c) passed the payment requests to the payments section for proces sing during the period of his employment;

(d) by gaining access to a data reception point within his former de partment outside normal office hours inserted fraudulent data into the system after leaving his employment.

The vouchers were drawn in favour of friends or associates, the cheques were cashed by these persons and the associates and the perpetrator divided the proceeds. As a result of the implementation of a new creditor payments computer system which necessitated new stationery being used, the last two fraudulent payment requests were queried and thus the fraud came to light.

Case 3: Amount: £14,000 Duration: 5 months

Perpetrator: Supervisor

The payments officer created unauthorised payments by submitting dummy invoices to the creditors system for which she was responsible, having previously set up a dummy creditors reference number. The cheques produced by the creditors system were sent to an address which she used to pick up the mail. Cashing the cheques was carried out via a building society account in a fictitious name. The Fraud was discovered as a result of budget monitoring and overspending on a budget head.

b) Output Frauds: Output frauds involve the suppression or alteration of data which emerges from a computer. In the one case reported to the Audit Commission, a finance officer responsible for the collection and control of rents misappropriated funds from these accounts and suppressed the computer balance reports which would have revealed the discrepancies. He was detected when he began altering input data as well. He was prosecuted and sentenced to four years' imprisonment. Some output fraud cases are:

Case 1: Amount: £1,000

Two thefts of presigned computer produced cheques occurred in the operations department of the computer area where presigned cheques are held in a safe awaiting processing. Number controls were exercised and the thefts detected but the culprit was not detected. Case 2: Amount: £229,185

Duration: 3 years

Perpetrator: Assistant operations controller

This fraud was committed on a Friday evening at a time when the evening shift of operators had left the computer suite without any authority and in breach of regulations, to go to the pub. The theft was timed at a bank holiday weekend when the majority of staff would not return to work until the following Wednesday, thus giving Saturday and Tuesday as days when cheques could be cashed without any alarm having been raised. The theft was detected when operations staff were unable to complete a payroll run because of a lack of cheques. The operations staff were the subject of internal disciplinary proceedings whilst the perpetrator of the theft was subsequently convicted and

given a prison sentence.

c) Program Frauds: The Audit Commission said that, while there was a feeling that a "true" computer fraud must involve the dishonest alteration of a computer program, in practice the evidence suggested that relatively few such frauds actually occur. The Commission noted that few program frauds may be detected because of the skill of the programmers in covering up the fraud, but considered that "... it seems unlikely that the quality of management throughout the international business world is so lacking that regular acts would continue to go unnoticed."

The programmer does have the opportunity to add instructions to a program which will only be activated when a "trigger" occurs, but most computer users are not programmers and are merely responding to the options which are provided by the computer system. In everyday use it is the ordinary user who has the greater opportunity dishonestly to manipulate a computer by altering the data which is keyed in. In an example of a program fraud given by the Audit Commission, two programmers designed a stock accounting system containing a hidden routine which on presentation of a certain password would suppress the volume of sales and thus reduce the liability of VAT payment.

The term "Computer Fraud" is used to mean the manipulation of a computer in order dishonestly to obtain money, property or some other advantage of value or to cause loss. There are no offences which correspond to the categories of input frauds, output frauds and program frauds because those categories relate to the manner of the commission of offences. The essence of these forms of conduct is similar to, and may be the same as, ordinary theft or fraud committed in some other way. In consequence, the existing offences of theft and fraud can be used to deal with most cases of computer fraud. The following are the main offences which fall for consideration here: theft, obtaining property by deception, false accounting and common law conspiracy to defraud.

Theft: Section 1(1) of the Theft Act 1968 states that a person is guilty of theft "if he dishonestly appropriate property belonging to another with the intention of permanently depriving the other of it;...".

When a computer is manipulated in order dishonestly to obtain money or other property, a charge of theft or attempted theft will generally lie. Such a

charge can be used, for example, in cases of input fraud where false data is entered by someone into a computer in order to obtain payments to which he or she (or another) is not entitled, for theft of money from a cash dispensing machine (ATM) using either a forged cash card or another's card, or for the theft of pre-signed computer cheques.

Obtaining property by deception, and other deception offences: Another possible charge, with the same maximum penalty as for theft, is obtaining property by deception contrary to the Theft Act 1968, section 15-"A person who by any deception dishonestly obtains property belonging to another, with the intention of permanently depriving the other of it,..." "Deception" is defined in section 15(4) as meaning - "...any deception (whether deliberate or reckless) by words or conduct as to fact or as to law, including a deception as to the present intentions of the person using the deception or any other person."

False Accounting: Section 17(1) of the Theft Act 1968 creates two offences, penalising anyone who-

(a) destroys, defaces, conceals or falsifies any account or any record or document made or required for any accounting purpose; or

(b) in furnishing information for any purpose produces or makes use of any account, or any such record or document as aforesaid, which to his knowledge is or may be misleading, false or deceptive in a material particular; in each case there must be proved to be dishonesty and either an intent to gain for himself or another or to cause loss to another. Both offences are punishable on conviction on indictment with seven years' imprisonment. The falsifying of accounts may be done in order to conceal the fact that an offence, such as theft, has taken place, but it may be difficult to identify the precise nature of the crime which is being concealed. The falsifying may itself be an integral part of a fraud, for example, an act of preparation for a fraud yet to be carried out. The use of a false or deceptive account may be an attempt to commit another offence involving dishonesty. Section 17 supplements both offences of theft and deception as well as offences of forgery.

Conspiracy to defraud: Conspiracy to defraud is a common law offence, the essence of which is - "... an agreement by two or more by dishonesty to deprive a person of something which is his or to which he is or would be or might be entitled [or] an agreement by two or more by dishonesty to injure some proprietary right of his..."

It is thus very broadly defined and makes possible the prosecution of a wide range of fraudulent conduct where two or more persons are involved. The offence is triable only on indictment and is punishable with a maximum penalty of ten years' imprisonment. Its use therefore tends to be limited to the more serious cases of fraud. From the point of view of its usefulness in relation to cases of computer fraud, one significant feature of conspiracy to defraud is the absence of any requirement of proof of detection or an intent to deceive. If two or more people agree by dishonest means to cause loss to another (for example, by obtaining property from them or valuable services) and their conduct involves or may involve the "deception" of a computer to achieve their objective, a charge of conspiracy to defraud could be brought against them.

CHAPTER 4: CONCLUSION

I have attempted to outline the dimensions of computer crime in the previous chapters. There is obviously a chaos in the subject as the inability of legislations to cope with less obvious kinds of computer crime has been proven. Where does this confusion originate from and is it possible to create such a system that will not leave any doubt for the definition of computer crime. In my view it is not possible to create a definition that will encompass all possible variations of computer misuse, as the intentionality of agents involved in a computer misuse can not be reduced to some formal structures (syntactical means) i.e. legislations that will produce a clear output in every different contextual situation. The Semiotic approach helps us to understand the dimensions of the problem in a better way in which we can analyze the system in four different levels: Pragmatics, Semantics, Syntactics and Empirics. Although I will give a brief definition of each level in relation to our concept of computer crime, it will still be far from a real application of semiotic framework as it requires a much more detailed academic work solely devoted to semiotics, which is not the aim of this study.

Pragmatic Level: The concept of intentionality in different contextual situations have always been the achilles heel of law and we come across with the same problem in a very obvious way in computer crime. Intentionality is the state of mind in any context but it does not necessarily mean that what we are doing is an exact reflection of what we think we are doing. This problem shows itself very clearly in the harmonization of legislations in different countries, the reason of which is that every culture has its own norms and the intentionality of agents in that culture are affected by the different norms that

govern them; therefore harmonization of legislation would also necessitate the harmonization of norms in the legislation which poses a very difficult problem.

Semantic and Syntactic Levels: The definitions we have come across in the previous chapters is a proof of the fact that there are many interpretations of the concept of computer crime. Every responsible agent operating in the domain of computer crime has an interpretation of the concept which may not necessarily be in accordance with the other definitions. The problem we encounter here also overlaps with the issues at the pragmatic level in which the intentionalities and norms affect the interpretation. But is it possible to separate the context at the pragmatical level and create a definition of computer crime that would be adaptive in every context? The answer to this question is `No' as there can't be an adaptive system semantics that will cater for all interpretations of computer crime in various contexts. What is the stage that we have come to then, are we on a standstill at this point? The answer to this question is also `No'. As we defined the concept of computer crime as a system and there is a continuous attempt to take the system under control while the system itself expands there will always be formal structures (syntactics) that tries to cover computer crime at the semantic level. These syntactical elements can be in the form of legislations, acts, private member bills etc. What we defined above is a current system boundary of computer crime but it always evolves and jurisdictions try to cover every evolving situation upto an extent but are not able to cope with the problems arising from intentionalities, contextual differences and different interpretations.

BIBLIOGRAPHY:

Audit Commission for Local Authorities in England and Wales, Computer Fraud Survey 1985.

Bequai, A., **TechnoCrimes**, Lexington, Mass.:D.C. Heath,1987

Computer-related crime: recommendation no. R(89)9...1990

Cornwall, H., **Datatheft**, London:Heinemann, 1987

The Law Commission, Working Paper No. 110, Computer Misuse.

Liebenau, J., Backhouse, J., **Understanding Information,** London: Macmillan, 1990.

Nicholson, E., **`Hacking Away at Liberty'**, The Times, 18 Apr. 1989

Norman, A.R.D., **Computer Insecurity,** London:Chapman and Hall, 1983

Nugter, A.C.M., **Transborder Flow of Personal Data within the EC.**

Parker, D., **Crime by Computer,** New York, Scribner, 1976

Sieber, U., **The International Handbook On Computer Crime,** New York: John Wiley, 1986.
Wasik, M., **Crime and the Computer,** 1991.
Law Reform Proposals on Computer Misuse [1989a]
Criminal Law Review 257.

Appendix A:

Ad A Exemptions from the whole of the act Excluded entirely from the operation of the DPA are personal data:

- held for domestic or recreational purposes;
- which the law requires to be made public;
- which safeguard national security;
- held for payroll, pensions and accounts purposes;
- from unincorporated members clubs;
- in mailing lists.

Ad B the non-disclosure exemptions
As a general exception to the thrust of the DPA disclosure is always permitted:

- to the data subject or with his consent;
- to employees or agents of the data user;
- to prevent crime or for taxation purposes;
- to safeguard national security;
- for legal purposes;
- in case of emergency.

Ad C the subject-access exemptions The right of access can be denied an individual:

- for the prevention of crime and for taxation purposes;
- for judicial appointments;
- where a legal professional privilege exists;
- to statistical or research data;
- to back-up data;
- to personal data held by a credit reference agency because here access is covered by section 158 of the Consumer Credit Act 1974;
- to data incriminating the data user, unless it concerns an offence under the DPA.

Ad D Modification of the right to accessBy order of the secretary of state in certain circumstances access can be modified in relation to:

- health data (section 29(1) DPA);
- social work data (section 29(2) DPA);
- data held by financial regulatory bodies (section 30(2) DPA);
- information protected by the law (section 34(2) DPA).

Appendix B:

- Rights of the data subject:

According to the seventh DP principle an individual is entitled:

(a) at reasonable intervals and without undue delay or expense
(i) to be informed by any data user whether he holds personal data of which that individual is the subject; and
(ii) to access to any such data held by a data user; and
(b) where appropriate, to have such data corrected or erased.
- Obligations of the data user:
(a) First principle:
"The information to be contained in personal data shall be obtained, and personal data shall be processed , fairly and lawfully".
(b) Second principle:
"Personal data shall be held only for one or more specified and lawful purposes."
(c) Third principle:
"Personal data held for any purpose or purposes shall not be used or disclosed in any manner incompatible with that purpose or those purposes."
(d) Fourth principle:
"Personal data held for any purpose or purposes shall be adequate, relevant and not excessive in relation to that purpose or those purposes."
(e) Fifth principle:
"Personal data shall be accurate and, where necessary, kept up to date."
(f) Sixth principle:
"Personal data held for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes."
(g) Eighth principle:
"Appropriate security measures shall be taken against unauthorized access to, or alteration, disclosure or destruction of, personal data and against

gued that re-arranging and evaluating have to be affected by means of other given features, which means that there would need to be a minimum of four features before there can be any question of `rearranging' or `evaluating'. In addition, the features should relate to the same file.

(e) Collection of document files: The aim of the German legislator was to restrict protection of personal data to organized and organizable data collections, for it is those to which access is easiest. Seen from this angle it is understandable that document files and collections of document files are excluded. By document file is understood a collection of carriers of written or spoken text and/or images created by a person or organization for a specific feature, in particular for the purpose of documentation, as records of administrative or commercial significance or in support of future decisions. The exclusion of(collections of) document files from the concept of file is of great practical significance

accidental loss or destruction of personal data."

(h) Obligation to register: Data users are under an obligation to register. Entry application shall contain
- the name and address of the data user;
- a description of the personal data to be held by him and of the purpose or purposes for which the data are to be held or used.

Appendix C:

Processing : Processing within the meaning of the BDSG embraces four phases:

(a) Storage: The acquisition, recording or retention of data on a storage medium so that they may be used again.

(b) Third-party disclosure: The passing of stored data or data acquired directly by means of data processing to third parties in such a way that the data are disseminated by the storage unit or are held ready for inspection, especially for retrieval.

(c) Modification: The alteration of the contents of the stored data.

(d) Erasure: The obliteration of stored data, irrespective of the methods used.

Personal Data: Details on the personal or material circumstances of an identified or identifiable physical person(the person concerned).

(a) Details: The intention to furnish information must be present.

The form in which the information is presented, whether digitally, in written form or on a sound tape, is irrelevant. Even an affirmative nod of the head can be information. Thus both automated and non-automated personal data are subjected to the BDSG.

(b) Personal or material circumstances: The German legislator employed the expression `personal or material circumstances' in order clearly to indicate that all information relating to a person falls within the act. Whether the piece of information in the particular case is personal or material in nature is not relevant.

(c) Identified or identifiable: A person is identified when it is clearly determinable from the data that they relate to that person. A person is identifiable when the person, although not able to be identified solely from that data, can be identified with the assistance of other information.

(d) Natural person: Every living individual is a natural person within the meaning of the BDSG.

Collected in a file: When information can be characterized as personal data there is still a formal requirement to fulfil,namely, that the personal

nal data intended for internal use.

(b) personal data intended for use by the media: The same exception is under (a) is made for the media, the reason lying in the fact that the regime of the BDSG could come into conflict with the freedom of the press and the freedom of expression.

(c) personal data in lists or otherwise compiled (non-disclosure exemptions): The disclosure to third parties of certain personal data in lists or otherwise compiled concerning members of a group of persons is not subject to the conditions laid down by the BDSG governing disclosure to third parties but remains only subject to the condition that the interests of the data subject concerned are not thereby prejudiced.

Appendix D:

(a) collection of personal data: Acquisition of the data by any fraudulent, dishonest or illegal means is prohibited.

(b) type of data that may be processed: Not all types of personal data may be processed. In the first place, processing the personal data of data subjects who have objected to their data being processed is prohibited. Secondly, personal data which directly or indirectly reflect racial origins or political, philosophical or religious opinions or union membership may in principle not be processed.

(c) the use of personal data: No governmental or private decision involving an appraisal of human conduct may be based on any automatic processing of data which describes the profile or personality of the person concerned. This provision thus constitutes a general prohibition on every data user from founding his decision-making process exclusively on automated personal data. This means that, for example, for credit organizations both approval and refusal decisions relating to loans on the basis of automated personal data must always involve a non-automated element.

(d) storage period: The storage time for personal data is limited by section 28 of the Act. This section provides that personal data may not be retained for longer than that stated in the declaration of processing submitted to the CNIL (Commission Nationale Informatique et Libertes), whose permission is required for an extension of that period. Following the expiry of the period the data may be retained only in anonymous form.

(e) obligation to register: Every data user is in principle subject to the duty to submit a declaration to the CNIL for each automated personal data re-

(d) Recording, arranging, rearranging, evaluating according to specific features: The data are recorded, in other words, are stored in a permanent and readable form. The concept of feature concerns the structure of a data collection. It is necessary to distinguish a formal abstract feature (for example,profession, height) from the substantive data (for example, lawyer, 1,71 meters). It is these concrete entries that constitute personal data within the meaning of the BDSG. Arranging means arranging according to a systematic order of succession or priority. Some argue that while the Act refers to arranging according to features, a minimum of two features needs to be present for arranging to take place within the meaning of the BDSG. A file containing, for example, only names would not satisfy this criterion. Equally, it is ar-

cording prior to processing. Processing for different purposes requires separate declarations to be submitted. By submitting the declaration the data user acknowledges that the processing shall be in conformity with the LIFL. The CNIL checks immediately upon submission of the declaration that all the required information has been furnished and, if so, issues a receipt. Only upon obtaining this receipt actual processing may begin. The declaration naturally does not relieve the data user from his responsibilities under the Act.

(f) duty to act in conformity with the declaration: The data user is under the obligation to act in conformity with the information which he supplied on the declaration form. This means that it is the declaration which determines the answer to questions such as what is the purpose of the recording, who is internally authorized to receive personal data, whether third-party disclosure is permitted, and so on. The processing of personal data for a purpose different to that stated in the declaration is a criminal offence.

(g) obligation to take security measures: The French legislator drew a direct relationship between the obligation to take security measures and the statement of purpose in the declaration. Respecting the statement of purpose is seen as the first requirement for security of personal data. The duty of security, which is ubiquitous in the LIFL, is,inter alia, expressed in section 29:

"Any person processing personal data or ordering such processing thereby shall undertake, vis-a-vis the persons concerned to see that all necessary precautions are taken to protect the data and in particular to prevent these from being distorted, damaged or disclosed to unauthorized third parties."