Computing and Security; a Task for the Lawyer?*

by H. Franken

Juridisch Studiecentrum 'Hugo de Groot', R.U. Leiden, Postbus 9520, 2300 RA Leiden, the Netherlands

INFORMATION MEANS POWER

Knowledge means power. So most of the hacker stories are success stories because of the respect people have for the lonely, young, intelligent, pale student who is too sharp for a multinational. Some high-school boys, working with cheap home computers, broke into the datacentre of the Chase Manhattan Bank by telephone. They came in using the free clients line and they tried various entry-codes. Once in the system, they changed all the entry-codes so that the bank could not reach its own data any more.

Another story concerns a prisoner in the USA, who was working on his resocialization-plan. He took a course in computing and succeeded in gaining access to the prison records. So while sitting in his cell, he changed the date of his release and was a free man two months earlier than he was supposed to be released.

In Holland hackers got into the central computer of the National Post Office where all the lists of secret telephone-numbers of ministers and police authorities are stored. Other hackers have manipulated bank computers getting away with millions of dollars. But it has also happened that schoolboys have manipulated radiation data in a hospital computer system. Such interference can be fatal, and then we are talking about attempted murder.

* Parts of this article are quoted from the report of the Netherlands Committee on Computer Crime, which I had the honour to chair. (SDU the Hague 1987).

ABUSE OF INFORMATION

Knowledge means power. Information means power. It is clear that information can also be used to hurt other people. Such abuse of information may happen by

- interruption of information systems
- violation of secrets
- manipulation of data.

We must all of us realise that nowadays information technology presents a new challenge to those who intend to abuse information or data. It is a challenge to hackers and to people who want to disclose and publish confidential documents. In addition modern information technology is a very powerful tool in the commission of well known crimes such as fraud, forgery and swindle.

DARK NUMBER

It is difficult to estimate the extension of the abuse of data in our information society. There are several reasons for this statement: First of all, how does one go about discovering computer abuse? It is a big problem. All the cases we know about are the result of a clear mistake by the offender and not of initiatives of the police authorities.

In the second place, it is not possible to categorise a great deal of the abuse of data within the existing types of offences recognized by the law. Thirdly, there is a problem in ascertaining any increase in the rate of abuse due to the lack of cooperation by victims with the police authorities. Many victims will not inform the judicial authorities for several reasons:

a. They fear that this will damage their company's reputation. Clients may get the impression that the company is not safe.
b. The victims are afraid of the way the judicial authorities behave. Policemen are not yet accustomed to investigating computer crimes and they may cause damage to the business. Shutting down the information system, or seizing tapes may cause chaos in the administration or production process.
c. Another reason for not informing the authorities is that the victim often prefers to obtain reparation from the offender for the damage caused rather than to suffer the loss and put the offender in jail.

INCREASE OF ABUSE

Although we are confronted with a lack of research results about the dark number of abuses of modern information technology, we cannot avoid the conclusion that there has been an increase in the number and variety of these abuses. The more sophisticated the technology becomes... the more sophisticated the crimes become. In recent years we have seen an increase in the daring of the abuser, who has little fear of being discovered. And what's more: an important increase in the total losses has taken place.

It is also clear that the range and type of victims has already become very wide. All sorts of businesses, governmental departments and private individuals have been affected.

It is also interesting to note that we can find future offenders in groups of criminals cooperating with whizz kids and computer professionals. And: A recent Swedish study reports that the number of female offenders is almost the same as that of male offenders. That is really unusual in criminology! – a result of emancipation!

Looking to the future we can be sure that the abuse of computers will increase not only because of the continuity of the trends I have already mentioned, but also because of a favourable trend in technological developments. The hardware and software are designed to be user friendly.

This notion of 'user-friendliness' is an important selling point, yet we must be aware that it also contributes to the decline of computer illiteracy. User-friendly interfaces enable a broader section of the public to use modern information technology which also means that criminally minded people will have access to it, too. Furthermore, we know organizations and institutions are becoming more and more dependent on electronic data processing, and that in turn means an increasing vulnerability in the way all our organizations – our social structures – function.

COUNTERMEASURES

What can we do against these abuses of information or data? There are several ways in which to protect ourselves against the interruption of systems, breach of confidence and manipulation of data.

First, preventive measures can be taken to reduce the risk of damage. These measures concern not only defects in hardware and software, and take into account the faults of owners and personnel, but also affect unforeseen risks, such as accidents and misuse by the owner's own personnel as well as by outsiders. We can divide the preventive measures for risk avoidance into four basic categories.

They concern:

- physical measures (as a safe place in the building);
- organizational measures (such as separation of functions between designers, operators and controllers);
- logical measures (such as protection built into the program itself – encryption modules, for example);
- legal measures.

The last category refers particularly to the transfer of risks to third parties. It may sound rather cynical but this is a task for the private lawyer. In all stages of the contact between sellers and buyers, and during the whole period in which a person uses computersystems, he has to be aware of risks he can put on the

shoulders of another person or company. This can be achieved through negotiations with one's partners in business or with one's employees, for example by inserting competition clauses, or by buying security from insurance companies or specialized agents such as escrow firms. I mention this because we must be aware that the legal solution of the problems of risk should be solved in the first resort by measures initiated by the private persons themselves. My main subject in this article, however, concerns the possible measures a government can take. But these measures will not have sufficient effect when the citizen or company does not act at a private law level also.

GOVERNMENTAL ACTIONS

Now let us look at the task of the government. Government has a powerful tool, called legislation. But here there's an inherent conflict. On the one hand we acknowledge the fundamental principle of the free flow of information, on the other hand society demands protection of data. The European Convention on Human Rights guarantees the freedom to receive and to gather information. It also provides for legal rules which must be made to protect data concerning health, reputation, privacy and the rights of others. Several countries have already passed legislation on this subject, while others are still at the discussion stage. Here finally we see that the Organisation for Economic Cooperation and Development has declared in late 1986 that in almost all member countries, governments and courts are confronted with a new kind of criminality. This criminality shows the same characteristics in all countries and therefore similar measures are required to avoid the creation of computer crime havens and to protect countries from becoming victims of such criminality of foreign origin.

For these reasons national legislation should be made to combat the following acts:

a. The input, alteration, erasure and/or suppression of computer data and/or computer programs made wilfully with the intent to commit an illegal transfer of funds or of another thing of value;
b. The input, alteration, erasure and/or suppression of computer data and/or computer programs made wilfully with the intent to commit a forgery;
c. The input, alteration, erasure, and/or suppression of computer data and/or computer programs, or other interference with computer systems, made wilfully with the intent to hinder the functioning of a computer and/or telecommunication system;
d. The infringement of the exclusive right of the owner of a protected computer program with the intent to exploit the program commercially and put it on the market;
e. The access to or interception of a computer and/or telecommunication system made knowingly and without the authorization of the person responsible for the system, either (i) by infringement of security measures or (ii) for other dishonest or harmful intentions.

The *OECD* view is that the criminal law should cover these types of conduct. The question is: can we combat this behaviour with the criminal law? The answer is no: the present provisions of the criminal law are no longer sufficient. We have several arguments for this statement.

1. In the statutes of many countries the offence of forgery is formulated in terms of counterfeiting a document. Forgery concerns falsely changing a message that is embodied in a durable way. But how does one treat the falsification of a computer program which is not embodied on a material carrier?
2. In respect of most fraudulent acts the act of a human being is essential. But realize: when a manipulated smart card is inserted in the petrol pump: who has delivered the gas? The machine has been manipulated and not a person. As a consequence this does not constitute fraud under the legislation of the most European countries. The legal definitions concern acts by a human victim and not by a 'machine victim'.
3. A rather prosaical argument. The punitive measures of the present statutes are too low to deter computer crime. In the Netherlands a swindler can get a maximum of 3 years in prison. A thief or a forgerer can get at most 4 years of detention. Another rule provides that one third of the punishment may be remitted for good behaviour in jail. So when his profits are several million guilders and the costs are only two or three years in prison then the overall profit will be a real incentive, certainly when it is gained tax free!
4. Another argument for the adaptation of the present criminal law: there are new types of behaviour which deserve penal sanctions that are not provided for in the present regulations: for example hacking, tapping of data communication, and data manipulation – such as the case of the prisoner who freed himself 2 months prematurely.
5. The next point has been the subject of debate between lawyers for several years. Our present statutes concern the property and loss of material 'goods' and especially formulated rights. The latter are protected by copyright or patent law. However 'goods' normally correspond to material objects. It is necessary to consider whether information or rather, data may be deemed a 'good' within the meaning of the law.

In the event of this question being answered in the affirmative, then data would be accorded protection on the basis of provisions in force regarding theft, embezzlement, criminal damage and the like. My opinion is *that data cannot be deemed a 'good'* and that consequently definitions of offences in which the term 'good' occurs have no bearing on data. As this conclusion may appear to be in conflict with some recent legal judgements in Belgium and the Netherlands, I shall give you the reasons for reaching this opinion.

ARE DATA TO BE CONSIDERED GOODS?

On October 1983 one of the Dutch Courts of Appeal decided a case of a man who copied software from a data carrier belonging to his employer onto a data

carrier belonging to him. He subsequently resigned and started up his own business in the same field as his employer. He made use in his business of the software which he had copied which, he admitted, saved him six months of research and development.

The Court of Appeal held that there was sufficient evidence in law that the accused had made unlawful copies of certain computer data which did not belong to him. The Court assumed that these data could be deemed to constitute a good within the meaning of the law, and that they were therefore capable of being embezzled.

The reasoning which led the Court to reject the defence argument that this case did not involve goods as defined by the law was the same as that used by the Dutch Supreme Court in 1921 in the ruling known as the Electricity Judgement. This judgement held that *electricity* is a good because:

- it cannot be denied that electricity has a certain independent existence;
- this energy can be transported and accumulated;
- this energy represents a certain value to the person who generates it, on the one hand because it takes money and effort to obtain it, and on the other hand because this person is in a position either to use this energy for his own purposes or to transmit it to others in return for remuneration.

The Court of Appeal adopted this line of argument in the case of computer data: these are also available, transferable and reproducible and possess an economic value, so that they, like electricity, can be deemed a good.

This development would appear to constitute a further step in the evolution of the concept of a 'good' from a purely physical, tangible object to include intangible things, from the material to the immaterial, from property object to property value. The question remains, however, as to whether this tendency is to be applauded. I feel that this stretches the meaning of 'good' too far, in such a way that it also embraces things which differ too greatly from material objects and on account of this ought to be dealt with in a different manner.

It cannot be denied that both data and material goods are transferable, reproducible, available and sometimes possess economic value. However, there are obvious differences. Goods (which also includes electricity) are the product of physical labour, while data are the product of mental effort: data, after all, often reflect or embody knowledge.

In addition to this, goods are *unique*: ownership or possession of these goods implies that others are denied the ownership or possession; data, on the other hand, are *multiple*: possession of them does not stop others also having possession of the same data. The act of copying does not deprive the legal 'owner' of any of his power - he continues to possess the data. It is not so much that he loses possession of the data, but he loses the *exclusive* possession of these data. It is my opinion that it would be going too far to extend the concept of 'goods' to include 'data'. Data, which are also taken to include software, are primarily intellectual products, to which other forms of protection should apply

apart from those which protect material objects. This conforms with the traditions, such as copyright and patent laws.

HOW TO CREATE NEW REGULATIONS?

New regulations are needed, but how can they be created? It does not fit with the status of a democratic society to let the work be done by the judge, who interprets by way of analogy the existing rules. No, this is a task for the legislator. But the legislator has to bear in mind that he can't use normal or traditional legal terms and concepts such as forgery, fraud, document, good. The legislator must also be aware that he can't use technical terms because they will become obsolete in a few months. There are many and rapid changes of concepts in the field of technology. The legislator has to look for new standards of behaviour. This is a potential field of research for the lawyer. I think these standards can be discovered through feedback mechanisms in which the interests which can be harmed are discovered. There are three types of interest which are at stake: availability, integrity and exclusivity.

The first interest concerns the *availability* of the means of storage, processing and transfer of data and of these data themselves (including software). The importance of uninterrupted access to these means and data increases in proportion to the degree of dependence of a society on these media and data.

The availability of means and data may be jeopardized by deliberate acts of malevolence such as sabotage, damage, destruction or removal of media or data, or the obstruction or interruption of data communications.

In order to achieve correct results and to be able to take the right decisions using data in computerized systems it is extremely important that these systems operate properly and that the data and programs are correct and complete. This is what is meant by the *integrity* of the systems and the data they contain.

If this integrity is undermined the result may be the disruption of production processes, the failure of the security systems of electricity generators or traffic control systems, or the payment of incorrect amounts in salaries or benefits, or any such potentially large-scale and costly malfunction.

Integrity may be damaged too by the falsification of data and software involving alterations, addition or removal of certain elements.

Having looked at the concepts availability and integrity, there is a third element. This involves the interest which companies, organizations and individuals can have in according data an *exclusive character*, for example because they do not wish unauthorized people to have access to secret or confidential information or because they wish to have exclusive control over how media and data are used and by whom.

In the first place the unauthorised possession, reproduction and dissemination of secret or confidential data may be considered prejudicial.

In addition to this there may be an interest in imposing restrictions on the *use* of particular data or media which are not in themselves secret or confidential. As they are the fruits of investment, it is understandable that there may

be resistance to the idea of third parties making use of the resultant products, for example by copying them or marketing them commercially without paying for them.

NEW OFFENCES

On the basis of the notions of availability, integrity and exclusivity the legislator can start his work. I had the honour to chair a committee charged with drafting a statute on this subject. In our draft we formulated new offences such as:

- disturbing data communication
- tapping data communication
- data manipulating
- computer trespass
- special rules for cheque cards

Apart from these rules for the behaviour of the citizen we need new areas of competence for the public prosecutor and the judge. We need the competence

- to receive and to gather information; that is to be able to search in a computer system.
- to decode a program; i.e. to oblige the system operator to give access, to enable the judge to oblige the operator to remove an encryption in order that the search may be conducted.
- to tap data communication for police purposes. At present the law permits the tapping of telephone conversations, but not the tapping of the communication of data in other ways. It is urgent that this lacuna is filled.

A THRIFTY HOUSEWIFE

A further statement must be made. It is an important point of judicial policy that a legislator has to behave like a thrifty housewife when it comes to making criminal law. This part of the law must be reserved for the last stage of control of the citizen, because it gives potentially wide reaching powers to the state. Through economical use of the criminal law my committee recommended that the unauthorized use of information technology equipment should not be penalized. An example of this behaviour is where employees carry out private work on their employers' computers.

Unauthorized use is not a criminal offence in many countries except in the case of 'joy riding'. 'Joy riding' can be distinguished from 'joy computing' in that it occurs in the public domain. In contrast, unauthorized use of computer media will generally occur in the non-public domain, so that it can be dealt with by means of internal disciplinary procedures. Where unauthorized use is carried out by an outside agent, this implies that unauthorized entry has been obtained. In that case we can't speak any more of the private character of the use of the equipment. When there are people from outside who try to get access without being authorized, we can speak in legal terms of computer trespass by analogy with the criminal offence of trespass of a dwelling, room or property. In defin-

ing computer trespass as a punishable offence we look upon the obtaining of unlawful access to computerized data-processing systems or those parts which are protected against intrusion. In my view it should only be a punishable offence if some form of security or protection against invasion is violated in order to secure unlawful access. Intrusion can be said to occur where a person obtains access without the consent of the authorized owner or user - this will can be demonstrated by words ('entry prohibited') or by deeds. In my opinion words alone are not sufficient. Words, such as a text on the screen stating that entry is prohibited for unauthorized persons, do indeed show an unambiguous desire on the part of the authorized controller, but do not exclude the possibility of entry by accident. This danger is far less great when a higher threshold is created, consisting of particular security measures to combat unlawful entry. This introduces a further restriction. The door must not only be closed, as it were, but also locked. The point at which the security measure is applied is then regarded as the border between the 'private domain' and the area that is open to the public. The background to this proposal is the belief that criminalization is necessary because 'computer trespass' as such is improper. The criminalization of such activity also creates an obstacle to harmful acts which might follow intrusion into computer systems (e.g. altering or erasing data, reading or copying confidential data). Subject to the necessary restrictions, the criminalization of computer trespass offers indirect protection to data in data processing systems.

THE CIVIL LAW

It is not only the criminal law that should be handled as a tool for impeding computer crime.

As well as the government, all branches of the private sector have an interest in a smoothly-running system of data management. The stipulation of rules pertaining to legal persons can provide a major stimulus to the creation of barriers to combat carelessness in protecting data flows. It is possible to imagine such a statutory regulation which could be introduced into the Civil Code. This might take a number of forms:

(a) as part of the annual auditing of the company accounts, the registered accountant would have to provide an assessment of the security of the computerized data processing systems used by the company;
(b) an expert (AC accountant or EDP auditor) would have to assess the reliability and continuity of the computerized data processing;
(c) a statement regarding the reliability and continuity of the computerized data processing would be included by the directors in the company's annual report; this statement would be assessed by the accountant.

In my opinion, the first variant (a security audit) is not to be recommended, at least at present. The accountants' declaration on the annual accounts is concerned with the question of whether these provide a faithful representation of the assets and the results of the legal person.

In this regard, automatic data processing systems are only examined in so far as this serves the aim of the audit. Under this variant much more would be expected of the accountant, namely an assessment of all the automated systems in the company. Irrespective of the cost factor, it is unlikely that the accountant would be able to provide an unconditional assessment of this sort.

At the second variant - a management letter by an expert - the problem arises, as to who can be considered competent as an AC accountant or an EDP auditor to provide the required assessment. In the absence of any regulation of the training of such specialists, it is impossible to indicate a group of people who can exercise this competence in such a way that the public can and should rely on their pronouncements.

We are left with the third variant. This involves the directors of the company incorporating a statement in the annual report as to the reliability and continuity of the company's data processing system. This would explicitly indicate that responsibility for the scope and quality of security rests with the directors. They would have first to indicate in writing the requirements which security in the company in question has to fulfil. Finally, the accountant can publicly state whether this declaration by the directors is or is not a true reflection of the facts by comparing it with a set of rules.

CONCLUSIONS

In conclusion, we can say: the rapid developments in information technology and telecommunications create uncertainty among those involved; it is unclear what *is* and what is *not* allowed. The law can serve a function in delimiting the border between what is permitted and what is not permitted. Such signposts clarify the situation. They can also help to create an awareness of the norms among those who come into contact with computerized data processing and data transfer, whether as system managers or as potential offenders. But a lawyer in these times has to be a modest man. Because the final conclusion to be drawn is that for various reasons the law should be invoked sparingly. If too great a weight is attached to the criminal law it becomes something of a 'paper tiger' - with plenty of pretensions but little scope for genuine enforcement. It is better to be less ambitious and to concentrate on what are seen as vital interests. This in itself is a reason for guarding against 'norm-inflation'.