Per Furberg[*]
Dealing with Computer Crime. A Critical Review of Legislative Reactions to Computer Crime

1 Computer crime

The development of information technology (IT) has opened up a whole range of new possibilities, enabling the storage and transmission of all kinds of communication. However, these new functions for information management have also brought with them new types of crime and the commission of traditional crimes by means of new technologies. Internet, websites and other communication facilities have made such criminal behaviour possible, independently of geographical limitations and national boundaries. The worldwide spread of computer viruses and similar malicious codes has provided proof of this reality.

These new threats are challenging existing legal concepts, cf. the description above in Part II, "Lawmaking and IT" of the dematerialisation in the IT-environment and its effects on current legislation. The use of metaphors from the "real" world is even more illustrative in the field of penal law, where the wordings and descriptions normally reflect views originating from a different technical culture.

Another problem is the useful and, outside the penal law, often recommended analogisms. According to the principle of legality, a criminal law provision may not be given a more extensive area of application than its wording permits. Legal measures to prevent and deter criminal behaviour must be clear, at the same time as the introduction of IT in almost every sector of daily life calls for a minimalist approach in order to avoid two different sets of rules and regulations depending on whether a transaction is supported by IT or executed in the traditional environment.

2 Legal harmonisation

National laws have gradually been adapted to IT, normally as a result of actions taken by various international organisations. Computer-related crime was discussed by an ad hoc committee of the OECD who in 1986 suggested a list of acts, which could constitute a common denominator between the different approaches taken by member countries. The work continued within the Council of Europe where expert committees elaborated recommendations on computer-related crime (N^{o}. R (89) 9) and on problems of criminal procedural law connected with information technology (No. R (95) 13). These reviews of European criminal laws and the recommendations to concerted actions formed the basis for the IT-related amendments in 1986 to the Swedish criminal law provisions regarding e.g. fraud, usury, unlawful use and breach of data secrecy (Government Bill 1985/86:65).

It is true that similar amendments were introduced in other European countries and resulted in a co-ordination of national penal law concepts, but only a binding international

[*] *Per Furberg* is a member of the IT Law Observatory. See presentation in Annex 1.

instrument may ensure the efficiency in the fight against these new phenomena. Consequently, the Council of Europe established a Committee of Experts on Crime in Cyberspace to provide such an instrument.

The committee carried out a comprehensive analysis of cyber-space offences and the new dimensions created by IT. The sometimes detailed considerations can be instanced with the special attention paid to the criminal law aspects of electromagnetic emissions radiating, for example, from monitors. In November 2001 the outcome of the committee's considerations – a Convention on Cybercrime – was opened for signature. It aims at harmonising the domestic criminal law in the area of cyber-crime, providing domestic criminal procedural law powers for the investigation and prosecution of such offences as well as other computer-related offences and establishing fast and effective international co-operation in this field.

In the following, some examples will be given of the corresponding domestic debate and the need from a legal perspective for a deep understanding of the prerequisites given by IT. The background is the findings of

- a committee, established by the Government, which in December 1992 issued the report "Information and the new **I**nformation**T**echnology – criminal and procedural legal aspects" (SOU 1992:110), and
- a commissioner (Jörgen Almblad), appointed by the government to consider the need for IT-related amendments in the aforementioned environment (Ju 1997:A), who tabled a memorandum of March 17, 1998, "Penal law and information technology – a basic inventory of the need for legislation".

3 Fundamental differences

The aforementioned committee started from a description of *data* and its character – demonstrating that the difficulty in understanding the IT-related legal issues is partly due to the fact that we are moving in the borderland between concrete and abstract objects. Some of the self-evident presumptions underlying a traditional viewpoint do not exist in the IT-environment. The committee assigned this digital category the term *quasi-material* and endeavoured to interpret or suggest amendments to the law, headed to avoid artificial concepts with too little attention paid to IT.

The commissioner, on the other hand, took his starting point in the traditional physical objects, and was apparently non-committal on the subject of technical IT-related issues. He found no need for any new specific criminal law provisions and recommended considering only a few minor amendments to the existing penal law. Other matters were to be solved within current legislation, according to the commissioner's findings.

None of these approaches have yet been adopted by the Swedish legislature, but most likely it will have to come to a decision as a result of the Convention on Cybercrime, which has been signed by Sweden and numerous other states.[1]

4 Documents

The penalty clause on falsification of a document is a good example of an area where the choice of approach to IT will be significant for future legislation and case law. The definition

[1] See http://conventions.coe.int/treaty/EN/cadreprincipal.htm

of “document” according to Chapter 14, Section 1 of the Swedish Criminal Code includes several “concealed demands” as a part of the word “document”. It is an implicit qualification within the document that it shall give *self-dependent existence* to the information and via its physical bounds provide a clear distinction from other physical objects. Additional demands to qualify a record as a document are that it must have certain *durability* and the ability to *convince of its authenticity*, i.e. to give the reader reason to believe that the document originates from the individual who, according to the document, is seen to be the originator.

The need for legal acceptance of signed electronic *data* formed the basis for the aforementioned committee, which focused on legal protection for the authenticity of electronic substitutes for traditional paper based originals. The commissioner, on the contrary, argued that criminal law protection emanating from such IT-routines was unnecessary and that it would be far-fetched to compare electronic signatures with traditional signatures. Instead the commissioner recommended an approach based on who could be regarded as issuer of the data *carrier*. When a record is transmitted, e.g. via electronic mail, the commissioner mentioned, as one possible solution, considering the sender as issuer of his hard disk and the addressee as the issuer of his storage *medium* – he should be regarded as “communicator of the information in its present state” on the computer where the received copy is stored. Further, the commissioner stated that electronic mail, deleted after being read by the addressee, has more in common with a conversation over the telephone than with traditional paper documents.

However, taking the issuer of the storage *medium* – furnished with numerous (signed) electronic messages – as starting point, would bring back an outdated approach and the penal sanctions would probably be fictitious as the user normally does not know on which physical disk the message will be stored, where it is held and who owns or otherwise has right of disposition of the data *carrier*. The protected interest is the need to be able to trust the statement on the origin of the text, not the genuineness of the disk drive. Many have not fully understood that all information is broken down to ones and zeros and that the unique aspect is related to a unique pattern of data rather than to unique physical examples; c.f. the implicit qualification within the document that it shall be an original.

A few years later the committee’s stress on the protection of *data* and its authenticity, more or less independently of its storage, was given support by the EC-directive (1999/93/EC) of the European Parliament and the Council on a Community framework for electronic signatures. Further, a contribution to the legal recognition of electronic documents has been given by the Convention on Cybercrime, which imposes an obligation to establish as criminal offence the input, alteration, deletion, or suppression of computer data, resulting in unauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic. The focus on the difference between data and the data carrier used to perform processing of the data is already evident from the convention’s choice of terms (Art. 1).

The principles of how to determine whether a record is authentic have for decades been a moot point of legal doctrine. The aforementioned commissioner’s statement – that it in principle does not matter whether the sender or receiver of a record should be considered the issuer of the copy stored on the receiver’s hard disk – is obviously not correct. In Swedish law, very simply, the authenticity of a traditional document is judged by asking who, according to the document, is the guarantor of the original physical example. If this information is true, the document is authentic.[2] This physical approach is not compatible with the quasi-material character of data and the Svea Court of Appeal has recently confirmed this by rejecting a count on document forgery consisting of issuing unauthentic telefax print-outs or electronic records

---

[2] This should not be confused with criminal acts committed by making false statements in an authentic document (cf. false certification, Chapter 15, Section 11 of the Criminal Code).

produced by word processing programs.[3] One may compare with German penal law, according to which the judge will have to decide who is the issuer of the *text*, a scheme compatible with IT and adopted for the Swedish laws on (signed) electronic documents for the customs and taxation legislation.

Consequently, the difficulty in adapting the legislation to the IT environment partly derives from the need to reconsider traditional legal concepts, debated even before the introduction of computers.

5 Protected electronic places

Another area where the approach to establish legal protection in the IT field will be especially decisive for the lawmaker is whether the criminal law protection shall be based on

- the existence and location of an electronic substitute of a certain physical place, the integrity of which is reserved for the possessor (spatial integrity) independent of the sensitiveness of the stored data, or
- the customary limitation in the IT environment to *immaterial* information as such independent of its storage space.

The difference between rules and regulations applicable to immaterial information on the one hand and a person's protected custody of digital data and documentary evidence on the other hand seems too have been neglected.[4]

This distinction, however, is reflected in the Convention on Cybercrime, ordering legislative measures to establish as a criminal offence unauthorised *access to* the whole or any part of a *computer system*. The protection of computer data is addressed in other sections of the convention. The survey of the European countries' penal laws, carried out by the Committee of Experts on Crime in Cyberspace, showed the Swedish choice of a divergent approach, namely that of giving legal protection by a penal provision regarding breach of data secrecy, formulated as unlawful *access to a recording* for automatic data processing. Should this provision be understood as a regulation regarding information as such or does it make certain methods of obtaining information a criminal offence?[5]

Another problem concerns the interpretation of the notion "unlawful". Is it meant to exclude liability when *consent* is given, when there exists a "lawful" dealing (e.g. statutory handling of protected information) or will this restriction have a bearing on the legal concepts of authority versus competence? Consider the example in chapter of a press reporter who hacks into a computer, pleading that the constitution relieves him of criminal liability.[6] Will the Swedish constitutional protection apply or will the criminal law protection be valid, regardless of the electronic environment?

The aforementioned commissioner has suggested two alternatives; (1) a criminal law protection of physical objects such as disk drives and (2) the protection of information as such. A report recently issued by a Swedish Governmental Committee tasked with considering the protection of personal data in working life has proposed that, as a general rule, there should be a ban on employers knowingly making themselves acquainted with the

---

3 Svea Hovrätt sentence of 31 May 2002, docket number B 5358-01.

4 See also my other contribution to this anthology, *Lawmaking and IT. Reflection on the Need for New Concepts and Categories of Thought*.

5 Cf. *ibidem*, part 2 on "Electronic places and digital bearers in the legal system".

6 Cf. *ibidem*, part 3.

contents of an employee's private electronic mail.[7] However, it is not clear whether the criminal code penalises such an act and to what extent, if any, an enactment of the proposal will have effect on the interpretation of the criminal code. Some employers state that they may read anything stored on their computers. Their adversaries refer to the Human Rights Convention and the Swedish constitutional protection from search of letters or other confidential items of mail and from secret wiretapping.

The aforementioned committee chose a more complex approach, covering the protection of data carriers, data representing (immaterial) information and the (virtual) "custody", analogous to traditional physical places of storage.[8]

6 Closing lines

It is necessary to clarify to what extent (virtual) electronic places and electronic instruments are protected by criminal law and to tie the legal protection to the infrastructure in cyberspace. Technical and administrative solutions to these needs are already in place, by way of passwords, cryptographic procedures to furnish with strong authentication of users, advanced electronic signatures, digital rights management systems, and the like.

The taking of physical objects as a starting point, as suggested by the commissioner, will strike a discordant note with the actual usage of IT. The new dimensions created by IT and the virtual substitutes for traditional instruments and closed places of storage need to be taken into consideration by the legislator and in case law, to give legal effect to the borderlines and protecting mechanisms already accepted by the users of IT.

---

7 Personlig integritet i arbetslivet, SOU 2002:18.

8 See *ibidem* part 2 on electronic places.