"Informatica e diritto", Vol. XVII, Prima serie, 1989, n. 1-3, pp. 55-61

Computer Evidence in the Continental Criminal Procedure: Some Admissibility and Proof-taking Issues

Davor Krapac

SUMMARY: 1. *Introductory remarks.* – 2. *Obtaining computer evidence: Admissibility tests in the continental law.* – 3. *Presentation of computer evidence: Limitations of the prosecutorial "freedom" of evidentiary burdens.* – 4. *Evaluation of computer evidence: a nced for expert knowledge limits the principle of the "free evaluation of evidence".*

1. INTRODUCTORY REMARKS

It is well known that in the science of the procedural law questions concerning evidentiary issues are of paramount importance because proof-taking is what one calls "I ame du proces", *the soul of the law suit* (Perrot, 1983, 95). The use of computer evidence in computer crime cases as well as other "classical" evidence within the scope of computer media, such as system manuals, computer run books, program documentation, data and program input forms etc. has brought new considerations for procedural law, because the existing evidentiary rules give few or no answers to various questions such as those of admissibility, expert testimony, discovery etc.

These questions have great practical significance. It is obvious that the phenomenon of computer crime poses a new threat to industrial societies which are more and more dependent on computer technology: by some estimates at the beginning of the eighties, one out of forty computer centres was affected by computer crime and its losses were much more severe than those in traditional crime (Sieber, 1986, 3 et seq; 29 et se.). Therefore, in view of the large "dark figure" in this field, every successfully tried computer crime case seems to be of importance for implemenring criminal policy of the contemporary increasingly computerized state.

A comprehensive study of these evidentiary questions is still missing. This is not surprising to those who are aware of the numerous difficulties in the field of the comparative law: one may consider only problems that arise in connection with the comparison of law governing factfinding activities in the common law and the civil law systems. These activities depend on various "evidentiary styles", complex law on evidence and are marked with disparity between the law in the books and actual practice (Damaška, 1973, 509.

Therefore, only a modest attempt to provide a brief sketch of some evidentiary questions can be made here. This survey will be limited to the criminal proceedings in the continental law, in particular to the three characteristic phases of the adjudicative factfinding activities: the obtaining, presentation and evaluation of evidence.

However, before this attempt a short preliminary remark on the notion of the "computer evidence" should be made.

A computer can store and reproduce information as well as perform certain tasks by handling data in a way which is beyond certain special abilities of man (Andrews, 1983, 44). Therefore its output – whether it is computer stored or computer generated data – differs significantly from other types of "classical" evidence, such as admissions of persons, testimonial evidence, documentary evidence etc. By this characteristic it obviously presents a new type of evidence and for the continental adjudicator poses two important questions: whether is it generally admissible to introduce it in criminal proceedings and whether it has enough credibility and probative value.

As to the former question, the answer is generally positive. The continental law is based on the principle of "free introduction and evaluation of evidence" (Sieber, 1986, 110). It means that all kinds of evidence, in view to its cognitive value, may be used in factfinding process. A certain exception could be found until recently in the French civil law, where the content of a document could be regarded as a "copy" with the consequence that the court might inquire into the underlying data (Amory, 1985, 341 et seq.) what in regard to computer evidence seemed to be impossible because of the judges ignorance of subspecialities of the computer field (see *infra*, 4).

As to the latter question, the answer depends on the requirements relating to a foundation of computer evidence. In the continental systems these requirements are not fixed by the rule of codified law, because such norms would be regarded as the rules of legal proof which would run against the principle of the "free evaluation of evidence" reffered to above. Rather, they must be established through court practice. We shall examine them briefly in the third section of our discussion.

2. Obtaining computer evidence: Admissibility tests in the continental law

It is well known that the legal regime of obtaining evidence depends generally upon the underlying "evidentiary style" in a particular procedural system. In the continental law systems, where the so-called "non-adversary" or "inquisitorial" criminal procedure exists, the investigating authorities can obtain evidence from computer record in two principally different ways.

Firstly if they can positively identify a particular computer, the documents

to be obtained and their detentors, they can request the latter to surrender these evidence, provided that the detentors are not defendants or privileged witnesses themselves. This case should present no obstacles in obtaining computer records because their detentors are under legal duty to comply to such request and can be legally compeled to fullfil it (see e.g. the so-called *Herausgabepflicht* in par. 95 of the CPP of the FR of Germany).

Secondly, if investigators of computer crime do not know the "whereabouts" of the computer evidence, a search of a computer centre or a computer terminal location and a seizure of the computer evidence may be needed. In that case, some questions may arise. They concern: *a*) the rules governing the performance of the exigent procedural acts and *b*) protection of certain legal interests such as privileged ties of particular persons to the defendant and protection of personal privacy.

a) The rules governing performance of the exigent procedural acts have great practical importance in computer crime cases because here there is a high degree of ease with which both instruments and fruits of the crime can rapidly destroy or alter computer evidence (Computer Crime, 1979, 100). This means that even prior to the formal opening of an investigation, a necessity to impound temporarily computer documents, conduct searches of persons and dwellings may arise. In the continental systems it is usually the police who are vested with these powers and exercise them *ex officio* or upon a public prosecutor's request. As the continental police usually have ample powers to perform warrantless searches and seizures, many questions regarding e.g. the drafting and execution of the warrants do not appear here, like in common law systems.

b) But some issues in connection with protection of certain citizen's rights may arise here. They are the rights of privacy and some other constitutionally guaranteed individual rights, whose violation may render obtained computer evidence inadmissible at the main trial.

A recent comparative study on the exclusionary rule in the FR of Germany has shown that although the violation of the statutory provisions on search and seizure does not *per se* lead to the suppression of evidence, this may occur when the trial court determines that permitting its use would violate the two judicially recognized constitutional principles which govern search and seizure in that country, the *Rechtsstaatsprinzip* (similar to the concept of "due process") and the principle of proportionality, *Verhaeltnismaessigkeit* (Bradley, 1983, 1039). The evaluation of the committed irregularities in search and seizure can bring a German court to the exclusion of evidence either in order to preserve the so-called purity of the judicial process (e.g. if a unconstitutional search had been accomplished through brutality or deceit which violated the *Rechtstaatsprinzip*) or in order to protect the individual privacy which outweighs the societal interest in the presentation of relevant evidence (e.g. if a seizure was a source of some evidence the use of which would condone unjustifiable intrusions in citizen's privacy rights; the principle of proportionality; Bradley, 1983, 1042).

Similar legal attitudes can be found in other continental countries. The French principle of the "loyauté dans la recherche des preuves" leads to the exclusion of evidence obtained through means which intrude the physical integrity of persons or the privacy rights (Bouzat, 1964, 162). The French courts weigh the impact of the violations of these rights against the rights of defense and in particular cases suppress the illegally obtained evidence. This system can be found also in some other countries with French legal tradition. In Yugoslavia, according to the dominant theory, evidence obtained through perpetration of a criminal offence should be inadmissible and excluded from the file before the main trial (art. 83, 269, 279 CPP).

Therefore, in continental systems as well, prosecutors and investigating authorities will sometimes have to face a situation where the operation of the exclusionary rules tend to "destroy" their case. Such cases will be in practice less frequent as in common law systems. But nevertheless, the continental prosecutors must be aware of this possibility, particulary in cases where public interest, seriousness of the crime and other extrajudicial circumstances (imagine a case of a big computer fraud or embezzlement!) exert pressure to speed-up the proceedings.

3. Presentation of computer evidence: Limitations of the prosecutorial "freedom" of evidentiary burdens

The main feature of the continental "non-adversary" trial is that the official inquiry is directed by the judge who is expected to examine *ex officio* all aspects of the criminal event and therefore authorized to determine which evidence will be taken during preliminary and adjudicative phases. The parties activities are here reduced to introduction of only those evidence which have not been presented by the judge himself.

This situation may lead to a conclusion that the continental prosecutor will have little difficulties in presenting his case since it will be the judge who will see to the completion of the relevant evidence and its presentation at the main trial. But two limitations to this "freedom" of the prosecutorial evidentiary burdens apply here: *a*) the defendant's right to inspect the file, which can undermine investigative efforts to elucidate deviations associated with a suspected computer crime and *b*) the so-called negative rules of legal proof, which in cases of particular crimes may affect the presentation of computer evidence by requirement that it should be presented only through expert testimony.

a) Various computer-related crime methods are sometimes very difficult to detect and prove because their perpetrators use programs which leave no evidence of changes to the computer programs and/or data files. The traces of such acts can be often discovered only with the help of the qualified expert for the particular computer system. Even then the detection process

may last pretty long and be very vulnerable to various intrusions from outside. Also, once discovered and collected, data on such crimes, if disclosed to perpetrators in an early investigation stage, may significantly enhance false defense strategies and even offer collusion possibilities.

Police and public prosecutors, who are the first state authorities notified on a suspected computer crime, have to secure the computer facility as the crime site, determine what printouts and other materials should be collected. But once collected, these materials will be in the investigation stage at the defendant's or his counsel's disposal to examine them, since in some liberal continental systems this procedural right has been guaranteed to them at this early stage of proceedings (e.g. art. 73 and 131 of the Yugoslav CPP). Therefore, prosecuting authorities will sometimes have to make a difficult choice at the formal initiation of the proceedings: either to introduce all obtained computer evidence at this moment to prove the grounds for the commencement of the proceedings or "withold" sensitive parts of it for a later stage and take risk of the improper investigation.

b) If a computer was use as an instrument of the crime (e.g. for a financial embezzlement) in some procedural systems a necessity for expert testimony may arise. In those systems it may be namely required that the facts of planning and controlling of the embezzlement must be established through examinations of books of accounts and transactions. These examinations can be carried out only by experts. In such a case, the public prosecutor or a judge will not have the full "freedom of the introduction of evidence" but will be rather bound to a particular sort of proof. Here computer records will serve as the basis for expert testimony and the traditional and well known questions of its procedural regime apply (e.g. the functions of expert witness, qualified persons, experience and sufficient degree of knowledge etc.).

4. Evaluation of computer evidence: a need for expert knowledge limits the principle of the "free evaluation of evidence"

The continental principle of the "free evaluation of evidence" which comes historically from German law, means that the adjudicators are free from legal rules regulating the weighing or credibility of evidence. According to this principle, the probative value of the particular evidence depends on the adjudicator's subjective evaluation. But this evaluation is not a process of the pure free-wheeling mind but rather a mental activity which must undergo a set of logical and rational criteria which have to be exposed in the written grounds of the judgment (test of trustworthiness and test of the probative value of evidence).

In the evaluation of computer evidence, solving these two tests will be affected by judges lack of knowledge in regard to computer programming, system design and other specialities of the computer technology. Consider

only the issue of checking the computer evidence trustworthiness: to establish it, adjudicators must resolve three principal questions: *a*) the type of the computer equipment and principles of its operation; *b*) who, when and how retrieved data from the computer and *c*) what was the information fed into the computer and how it was processed. Or, consider the issue of the standards of proof which has been traditionally set very high in the continental doctrine (continentals will say that the adjudicators must attain the subjective state of full certaintly of the existence of guilt before convincting, expressed by the maxim *in dubio pro reo* which corresponds to the requirement of the proof "beyond a reasonable doubt" in the common law). How will judge and his lay colleagues in the mixed panel draw inferences from computer evidence, which are to be drawn according to rules of the particular specialty, unknown to them?

It is obvious that the practical "freedom" in evaluation of computer evidence will be minimal and that the court will have to use expert testimony to resolve many questions also in this stage of proof taking. But even in doing that, the court will not be able to evaluate it completely, because his "freedom" extends only to that part of the expert testimony for which the presuposed knowledge of computer technology is not required. This is however, a smaller part of it. The larger one, founded upon the knowledge of this technology, will have to be accepted by the judges without satisfying completely their cognitive needs or to be abandoned altogether.

This problem can be possibly solved only by rising the quantum of the judge's degree of knowledge of the computer technology. This could help articulate standards on proof-sufficiency for guilt determination in computer crime cases. Theoretically, this solution can be attained in two ways: "externally" and "internally". "Externally", by using the so-called "expert-consultants" in criminal proceedings (not only as the assistants to the parties as e.g. in the art. 323-325 of the Italian CPP but also as assistants to the court, such as in art. 168 of the Yugoslav CPP or in art. 133 [1] of the CPP of the Russian Soviet Federative Socialist Republic). "Internally", by staffing court panels with lay adjudicators who have a certain degree of knowledge of computer technology. Thus specialized tribunals for computer crime would be *de facto* created. But in view of the ongoing specialization in the particular fields of criminal justice (e.g. juvenile justice, panels specialized for economic crimes, taxation courts etc.) this may, under certain procedural safeguards, be the most acceptable solution.

REFERENCES

BERNARD AMORY, *Le droit de la preuve face a l'informatique et a la telematique*, «Revue internationale de droit comparé», 2, 1985.

DAVID ANDREWS, *The Legal Challenge Posed by the New Technologies*, «Jurimetrics Journal», Fall 1983.

PIERRE BOUZAT, *La loyauté dans la recherche des preuves. Problémes contemporains de procedure penale*, Institut de droit comparé de l'Université de Paris, 1964.

CRAIG BRADLEY, *The Exclusionary Rule in Germany*, «Harvard Law Review», Vol. 96, 1983.

Computer Crime. Criminal Justice Resource Manual, U.S. Department of Justice, Bureau of Justice Statistics, 1979.

MIRJAN DAMAŠKA, *Evidentiary Barriers to Conviction and Two Models of Criminal Procedure: A Comparative Study*, «University of Pennsylvania Law Review», Vol. 121, *3*, 1973.

ROGER PERROT, *Le droit a la preuve*, The general report for the VIIth International Congress on Procedural Law, Würzburg, 1983.

ULRICH SIEBER, *The International Handbook on Computer Crime*, Chichester, New York, 1986.