Recommendation No. R (95) 13

of the Committee of Ministers to Member States

Concerning Problems of Criminal Procedure Law Connected with Information Technology

(Adopted by the Committee of Ministers on 11 September 1995
at the 543 meeting of the Ministers' Deputies)

The Committee of Ministers, under the terms of Article 15.b of the Statute of the Council of Europe.

Considering that the aim of the Council of Europe is to achieve a greater unity between its members;

Having regard to the unprecedented development of information technology and its application in all sectors of modern society;

Realizing that the development of electronic information systems will speed up the transformation of traditional society into an information society by creating a new space for all types of communications and relations;

Aware of the impact of information technology on the manner in which society is organised and on how individuals communications and interrelate;

Conscious that an increasing part of economic and social relations will take place through or by use of electronic information systems;

Concerned at the risk that electronic information systems and electronic information may also be used for committing criminal offenses;

Considering that evidence of criminal offenses may be stored and transferred by these systems;

Noting that criminal procedure laws of members states often do not yet provide for appropriate powers to search and collect evidence in these systems in the course of criminal investigations;

Recalling that the lack of appropriate special powers may impair investigating authorities in the proper fufilment of their tasks in the face of the ongoing development of information technology;

Recognising the need to adopt the legitimate tools which investigating authorities are afforded under criminal procedure laws the the specific nature of investigations in electronic information systems;

Concerned by the potential risk that member states may not be able to render mutual legal assistance in an appropriate way when requested to collect electronic evidence within their territory from electronic information systems;

Convinced of the necessity of strengthening internation co-operation and achieving a greater compatibility of criminal procedural laws in this field;

Recalling Recommendation No. R (81) 20 of the Committee of Ministers on the harmonisation of laws relating to the requirement of written proof and to the admissibility of reproductions of documents and recordings on computers, Recommendation No. R. (85) 10 on letters rogatory for the interception of telecommunications, Recommendations No. R (87) 15 regulating the use of personal data in the police state and Recommendations No. R (89) 9 on computer-relating crime,

Recommends the governments of member states:

i. when reviewing their internal legislation and practice, to be guided by the principles appended to this recommendation; and

ii. to ensure publicity for these principles among those investigating authorities and other professional bodies, in particular in the field of information technology, which may have an interest in their application.

Appendix to Recommendation No R. (95) 13

concerning problems of criminal procedure law connected with information technology

I. Search and seizure

1. The legal distinction between searching computers systems and siezing data stored therein and intercepting data in the course of transmission should be clearly delineated and applied.

2. Criminal procedure laws should permit investigating authorities to search computer systems and seize data under similar conditions as under traditional powers of search and seizure. The person in charge of the system should be informed that the system has been searched and of the kind of data that has been siezed. The legal remedies that are provided for in general against search and seizure should be equally applicable in case of search in computer systems and in case of seizure of data therein.

3. During execution of a search, investigating authorities should have the power, subject to appropriate safeguards, to extend the search of other computer systems within their jurisdiction which are connected by menas of a network and seize the data therein, provided immediate action is required.

4. Where automatically processed data is functionally equivalent to a traditional document, provisions in the criminal procedure law relating to search and seizure of documents should apply equally to it.

II. Technical Surveillance

5. in view of the convergance of information technology and telecommunications, law pertaining to technical surveillance for the purpose of criminal investigations, such as interception of telecommunications, should be reviewed and amended, where necessary, to ensure their applicability.

6. The law should permit investigating authorities to avail themselves of all necessary technical measures that enable the collection of traffic data in the investigation of crimes.

7. When collected in the course of a criminal investigation and in particular when obtained by means of intercepting telecommunications, data which is the object of legal protection and processed by a compuer system should be secured in an appropriate manner.

8. Criminal procedure laws should be reviewed with a view to making possible the interception of telecommunications and the collection of traffic data in the investigation of serious offenses against the confidentiality, integrity and availability of telecommunications or computer systems.

III. Obligations to co-operate with the investigating authorities

9. Subject to legal privileges or protection, most legal systems permit investigating authorities to order persons to hand over objects under their control that are required to serve as evidence. In a parallel fashion, provisions should be made for the power to order persons to submit any specified data under their control in a computer system in the form required by the investigating authority.

10. Subject to legal privileges or protection, investigating authorities should have the power to order persons who have data in a computer system under their control to provide all necessary information to enable access to a computer system and the data theirin. Criminal procedure law should ensure that a similar order can be given to other persons who have knowledge about the functioning of the computer system or measures applied to secure the data therein.

11. Specific obligations should be imposed on operators of public and private networks that offer telecommunications services to the public to avail themselves of all necessary technical measures that enable the interception of telecommunications by the investigating authorities.

12. Specific obligations should be imposed on service providers who offer telecommunications services to the public, either through public or private networks, to provide information to identify the user, when so ordered by the compentant investigating authority.

IV. Electronic Evidence

13. The common need to collect, preserve, and present electronic evidence in ways that best ensure and reflect their integrity and irrefutable authenticity, both for the purposes of domestic prosecution and international co-operation, should be recognized. Therefore, procedures and technical methods for handling electronic evidence should be further developed, and particularly in such a way as to ensure their compatability between states. Criminal procedural law provisions on evidence relating to tradition documents should similarly apply to data stored in a computer system.

V. Use of Encryption

14. Measures should be considered to minimise the negative effects of the use of cryptography on the investigation of criminal offenses, without affecting its legitimate use more than is strictly necessary.

VI. Research, statistics and training

15. The risks involved in the development and application of information technology with regard to the commission of criminal offenses should be assured continuously. In order to enable the competent authorities to keep abrest of new phenomena in the field of computer related offenses and to develop appropriate counter-measures, the collection and analysis of data on these offenses, including modus operandi and technical apsects, should be furthered.

16. The establishment of specialised units for the investigation of offenses, the combating of which requires special expertise in information technology, should be considered. Training programmes enabling criminal justice personnel to avail themselves of expertise in this field should be furthered.

VII. International Cooperation

17. The power to extend a search to other computer systems should also be applicable when the system is located in a foreign jurisdiction, provided that immediate action is required. In order to avoid possible violations of state sovereignity or international law, an unambigious legal basis for such extended search and seizure should be established. Therefore, there is an urgent need for negotiating international agreements as to how, when and to what extent such search and seizure should be permitted.

18. Expedited and adequate procedures as well as a system of liason should be available according to which the investigating authorities may request the foreign authorities to promptly collect evidence. For that purpose the requested authorities should be authorized to search a computer system and seize data with a view to its subsequent transfer. The requested authorities should also be authorized to provide trafficking data rtelated to a specific telecommunication, intercept a specific telecommunication or identify its source. For that purpose, the existing mutual legal assistance instruments need to be supplemented.