

EUROPEAN PARLIAMENT



SCIENTIFIC AND TECHNOLOGICAL OPTIONS ASSESSMENT

**STOA**

**THE USE OF NEW TECHNOLOGIES IN  
THE ESTABLISHMENT OF THE  
EUROPEAN JUDICIAL NETWORK  
(EJN)**

**Final Study**

Document de travail pour le Bureau STOA

Luxembourg, juin 1999

PE 167.956/Fin.St./EN

EN

EN

**Catalogue:**

Titre: **THE USE OF NEW TECHNOLOGIES IN THE ESTABLISHMENT OF THE EUROPEAN JUDICIAL NETWORK (EJN)**

Workplan Ref EP/IV/B/STOA/98/C 14/02

Publication: European Parliament  
Directorate General for Research  
Directorate A  
The STOA Programme

Auteur: **M. Eric Sutter - Bureau Van Dijk - Ingénieurs Conseil**

Editeur: M. Dick HOLDSWORTH,  
Head of STOA Team

Date: June 1999

numéro PE: **PE 167.956/Fin.St./EN**

---

This document is a working Document for the 'STOA Panel'. It **is** not an official publication of **STOA**.

**This** document does not necessarily represent the views of the European Parliament

---

**ACC 876**  
**April 1999**  
**Author: Mr Eric Sutter**

## Summary

**An** extremely wide variety of cross-border criminal networks are involved in illicit activities in all areas: terrorism, illicit trafficking in dangerous waste, money-laundering, computer crime, trafficking in goods, etc. Such networks are increasingly making use of the opportunities provided by the new information and communication technologies to misappropriate confidential data or to thwart the efforts of enforcement agencies. The activities of criminal networks are no longer confined within borders.

It is therefore necessary for the police and judicial authorities responsible for combating these types of crime to learn new skills, and for cooperation to become more systematic between magistrates and police forces in the various countries.

### **Different approaches**

The roles played by the Ministries of Justice and Home Affairs, the Public Prosecutor's Office, the judiciary and the police vary **from** country to country within the European Union. Specialised departments generally exist within the above bodies to deal with each category of crime, but in some countries, there are a large number of different bodies. This situation can make it difficult to find the right person to talk to and to exchange information effectively; it can also hamper efforts to cross-reference information on complex cases.

### **Judicial cooperation**

Unlike police cooperation, judicial cooperation is a new development at EU level. The main objective of the work being undertaken in the field of judicial cooperation in criminal matters is to establish a legal framework enabling investigators and magistrates from various Member States to cooperate in following up 'transnational' criminal cases.

On 29 June 1998, the Council established a structure called the 'European Judicial Network'. The network comprises a number of 'judicial contact points', i.e. intermediaries whose job it is to exchange information by various technical means, meet periodically and draw up documents or develop tools to facilitate cooperation between Member States.

Several contact points are appointed in each EU Member State, so as to speed up the exchange of information and to take account of the different situations in each country. Common tools are currently being developed: a list of contact points, concise legal and practical details regarding the legal and procedural systems used in each of the 15 Member States, in the form of data sheets, a compendium of agreements, declarations and reservations. This information will be made available to all magistrates in charge of cases involving organised crime, in the form of CD-ROM to be produced in mid-1999. The use of a 'secure' telecommunications network was judged premature, since for the moment it would be too costly and too much of a handicap for those contact points which do not yet have the necessary equipment.

### **The benefits of new technologies**

Computer technology can be used at various stages in the judicial process:

- administrative follow-up of criminal proceedings (this involves the recording of administrative data on each case as it develops)
- personal data (data on anyone with a criminal involvement in a case needs to be readily accessible).

- documents connected with cases (digitising the contents of documents, enabling them to be consulted simultaneously by several different people; consolidating information enabling 'computer-assisted investigation' systems to be set up).
- drafting and proper formulation of international judicial assistance documents (such as letters rogatory)
- as an aid to translation
- remote access to up-to-date legal documentation (national and foreign)
- statistics and flow management

**As** far as telecommunications technologies are concerned, fixed telephones have been in widespread use for many years and mobile telephones now allow people to get in touch with others or to be contacted wherever they are. Faxes, and more recently e-mail, are now widespread, enabling information (text, images and sound recordings) to be exchanged with one or more correspondents. Videoconferencing, on the other hand, requires greater resources, but allows the remote examination of witnesses and the remote consultation of experts.

Nevertheless, the degree of use of new information and communication technologies varies greatly from Member State to Member State. Some of the computer systems which exist were built several years ago and are based on 'closed' technology which hampers migration to more modern technologies, integration into larger systems and interconnection.

### **Common tools**

The most advanced tool that has been introduced as a result of the political will shown by the Member States to cooperate in this field is the Schengen Information System (SIS), on which agreement was reached in 1996 and which was set up the same year. It ensures the rapid dissemination of information on wanted persons and individuals under surveillance. It comprises files containing personal data together with administrative and legal information. It also covers certain types of goods such as works of art.

**As** yet no decision has been taken on the European Judicial Network system. National representatives rejected the idea of a dedicated telecommunications network for the EJM, on various grounds, such as the cost of a secure system and the fact that some contact points did not have computers. Thus far, it has not been deemed appropriate for Europol's computer resources to be used, given that Europol has a single contact point per country while the EJM has several. The decision on whether to move over to an Intranet or Internet server has been deferred until 1999-2000.

There is currently no provision for the exchange of operational information, for example, for data security reasons, there are no plans to disseminate evidence (on data security grounds). It has been decided that, provisionally, CD-ROMs will be used as a means of distributing documentation.

### **Obstacles standing in the way of action to combat cross-border organised crime**

According to the people we spoke to, at the moment the main problem inside the European judicial area is not technological disparities but disparities in national legislation (prevention, offences and crimes) and in legal traditions (relating to the concept of evidence and the right to use evidence).

Certain formal procedures (notification, etc.) have no place in action to combat crime. Some countries make no distinction between what comes under 'intelligence' and what comes under 'crime'; the necessary files exist, but there is no cooperation.

The fact that the Member States do not all use the same language constitutes a barrier to the exchange of information, even though people at a given level of responsibility might be expected to know at least one foreign language. Nonetheless, legislative texts, administrative documents, files and evidence are rarely available in more than one language.

In most countries, it is illegal to merge files containing personal data compiled by various departments and to forward that data without the consent of the person concerned.

Various files are compiled in each country by the police and judicial authorities. These files are often not available on line. Files compiled by the various police and judicial authorities are not always compatible, even inside a given country. Different bodies use different file structures, which makes consultation difficult, even in cases where it is authorised and appropriate. Furthermore, most existing files should be gradually transferred to open platforms, but that is a costly process.

In order for new technologies to be used effectively, the staff involved in legal cases must have both the necessary processing and communication equipment and the skills required to make the best possible use of these new tools. This requires both training and the simplification of the tools themselves.

### **Community action taken**

In order to prevent judicial action from being hampered by the current system's serious shortcomings in terms of efficiency and speed, improved knowledge of the judicial structures and procedures of all Union countries is essential.

The standardised information sheets on practices in the area of basic judicial measures in EU countries, which will be distributed on **CD-ROM** in June 1999 by the General Secretariat of the European Union, will improve knowledge of basic judicial measures and may be supplemented on regular basis so as to provide increasingly exhaustive, precise and up-to-date information.

Multi-annual exchange and training programmes (such as the Falcone programme) have been set up but so far only a small number of law officers have taken part in them.

Other programmes have also been set up on data protection.

## **Future action**

In the medium term, a European expert system should be set up, similar to that introduced in the Netherlands for letters rogatory to be sent abroad. Under such a system, guidance may be given to each Union country to enable it to draw up, in one of the agreed languages, and issue, letters rogatory intended not only for direct recipients in other Union countries but for countries throughout the world.

When an individual, who may or may not belong to an international criminal organisation, is suspected, accused or convicted of a serious crime or offence, the judicial authorities of the country concerned must be able to consult databases, some of which should cover the territory of the European Union, including:

- a national register for each country so that the identity of an individual can be checked (first and second names, date and place of birth, gender, nationality, domicile, etc.);
- a national criminal records database for each country for checking whether an individual has ever been convicted of a crime by the judicial authorities of the country in question;
- a central database for current legal cases to make it possible to find out whether, and in respect of what facts and with what accomplices, an individual is or may be implicated in another case at international level in the European Union, in order to examine the possibility of connections between cases and of the joinder of the new investigation inquiry.

The other information which must be checked such as the use of false names, finger prints, whether or not an individual belongs to an international criminal organisation, connected individuals, whether or not the individual is being detained, etc., is held in police or prison databases which have to be consulted by the police at the request of the judicial authorities.

Information concerning judicial measures is constantly changing since not only is it subject to modification but it also needs to be supplemented, clarified and made more specific. This would simply involve putting an Internet server on an existing Intranet network belonging to a European body such as Europol. The tools needed to ensure the security and protection of information distributed in this way already exist.

The documents relating to letters rogatory produced using an expert system should be distributed by e-mail on a European Intranet network rather than printed on paper, sent by fax and/or post.

Even the level of Principle Public Prosecutor's Office appears ill-equipped to combat cross-border organised crime and a single National Public Prosecutor's Office for each country would seem to offer a more effective solution. The National Public Prosecutor's Offices would be connected up through the Intranet referred to earlier and would have access to appropriate national databases. They would exchange information on current cases involving international criminals in their respective countries with a Principle Public Prosecutor's Office at European level to which they would submit proposals for joining certain ongoing cases, covering more than one country, on the grounds of the connections between them.





## CONTENTS

INTRODUCTORY REMARKS .....	5
1 THE NEW FORMS OF 'ORGANISED CRIME'.....	6
1.1 THE AREA COVERED .....	6
1.2 THE BASIC FEATURES OF THESE NEW TYPES OF CRIME .....	7
2 EXISTING ADMINISTRATIVE STRUCTURES .....	7
2.1 WITHIN THE MEMBER STATES .....	7
2.1.1 Different approaches .....	7
2.1.2 In some countries, there are a large number of different bodies .....	8
2.1.3 Involvement in supranational mutual assistance structures.....	10
2.2 AT INTERNATIONAL LEVEL .....	11
2.2.1 Interpol.....	11
2.2.2 The G8 .....	11
2.2.3 The Council of Europe .....	12
2.3 WITHIN THE EUROPEAN UNION .....	12
2.3.1 Police and customs cooperation.....	12
2.3.2 Cross-borderjudicial cooperation .....	13
3 EQUIPMENT AND TECHNICAL INFRASTRUCTURE.....	15
3.1 THE BENEFITS OF NEW TECHNOLOGIES .....	15
3.1.1 The benefits ofcomputer technology .....	15
3.1.2 The benefits of telecommunication technologies.....	17
3.1.3 Identification and authentication devices .....	18
3.2 THE CURRENT SITUATION IN THE MEMBER STATES .....	18
3.2.1 Overview.....	18
3.2.2 A few examples.....	19
3.3 AT EUROPEAN LEVEL.....	21
3.3.1 Common tools .....	21
3.3.2 Data exchange between judicial authorities.....	21
4 OBSTACLES STANDINGIN THE WAY OF ACTION TO COMBAT CROSS- BORDER ORGANISED CRIME .....	<b>22</b>
4.1 Differences in national legislation and practice.....	22
4.2 Cumbersome administrative procedures and lack of legal approval .....	23
4.3 Access to legal documentation .....	23
<b>4.4</b> Linguistic diversity.....	23
4.5 Data protection.....	24
4.6 Lack of access to files .....	24
4.7 File incompatibility .....	24
4.8 Inadequate staff training.....	24
<b>4.9</b> Territorial limitations.....	24
4.10 Computer evidence.....	24
5 COMMUNITY ACTION.....	25
5.1 Comparison of legislation and practice.....	25
5.2 Data protection.....	26
5.3 Training .....	26
6 A VISION <b>OF THE</b> FUTURE OF JUDICIAL COOPERATION.....	27
6.1 POLICE AND JUDICIAL COOPERATION ACTORS .....	27
6.1.1 Police cooperation.....	27
6.1.2 Judicial cooperation.....	27
6.2 LEVELS AND INSTRUMENTS OF JUDICIAL COOPERATION.....	27

6.2.1	Harmonisation.....	26
6.2.2	Knowledge of structures and practices in other Union countries and targeted judicial action.....	27
6.2.3	Databases containing information on criminals and criminal organisations.....	27
6.3	JUDICIAL COOPERATION TOOLS .....	27
6.4	THE STRUCTURE OF JUDICIAL COOPERATION.....	<b>28</b>

## **INTRODUCTORY REMARKS**

1. The 'European Judicial Network' is a rather ambiguous concept which needs to be more clearly defined in order to determine the terms of reference of this study. The term can be interpreted restrictively to mean the 'network of contact points' (a relatively simple structure) established in July **1998** by the Council of the EU. However, it may also be seen in the broader context of the 'European judicial area', owing to the fact that some countries see judicial cooperation, or what might be called 'cooperation in the administration of justice', as including police cooperation and any future European criminal authorities. We have opted for the latter interpretation, since it enables us to examine the background to the 'network of contacts', as well as future developments.

**2.** The contact points have little influence in the European Judicial Network proper, given that most decisions are taken within the Secretariat of the Council of the EU. Furthermore, only the magistrates concerned are supposed to have any knowledge of the establishment of the network, and the work being carried out is not supposed to be known to anyone 'outside' the network.

It would be difficult and, indeed, of little practical use to go into the issue of the technical resources to be used, until basic needs and the substance of what is to be exchanged, shared or made available have been determined, since the technical solutions to be used will depend on what is actually decided. We shall just have to wait until the working parties which have been set up publish their findings.

3. Information on the 'judicial area' - some of which is extremely scanty - has been received from only five countries (Spain, France, Italy, Finland and the Netherlands), despite the fact that several letters and faxes were sent to both the Justice and the Home Affairs Ministries of the various countries.

# 1 THE NEW FORMS OF 'ORGANISED CRIME'

## 1.1 THE AREA COVERED

Organised criminal activities are a growing threat to the security of both individuals and society as a whole. An extremely wide variety of cross-border criminal networks are involved in illicit activities in all areas:

- terrorism
- trafficking in firearms and explosives
- illicit trafficking in dangerous waste and nuclear, biological and chemical substances;
- money-laundering;
- financial fraud and fraudulent commercial transactions which damage the interests of both individuals and governments;
- computer crime;
- the counterfeiting of money and goods;
- trafficking in human beings, prostitution and procuring, paedophilia, and slave-trading;
- illegal immigration;
- trafficking in drugs and chemical precursors;
- trafficking in stolen goods, which covers thefts from financial establishments or security firms, theft of and trafficking in private cars and goods vehicles, theft of and trafficking in works of art, etc.;
- swindles and other types of fraud.

Nearly 90% of all cross-border organised crime is, either directly or indirectly, financial or economic (including drug-related crime, owing to the link with money-laundering). The frauds perpetrated are generally complex and multi-layered and involve swift transfers.

Such networks are increasingly making use of the opportunities provided by the new information and communication technologies to gain access to or misappropriate confidential data, coordinate the activities of their members, exchange information enabling them to thwart the efforts of enforcement agencies, circumvent the law, take advantage of legal loopholes existing in some countries, and so on. The financial resources of such networks and the know-how of some of their members enable them to make use of the most advanced technologies.

The term 'high-tech crime' basically covers two types of activity:

- using new technologies to commit 'conventional' crimes and offences;
- gaining illicit access to computer systems.

In the latter instance, sophisticated criminals gain access to computer and telecommunication systems so as to illicitly obtain or modify valuable data or to attempt to disrupt the smooth operation of commercial and public systems of critical importance.

## **1.2 THE BASIC FEATURES OF THESE NEW TYPES OF CRIME**

The different types of crime are becoming increasingly interrelated (for example, networks bringing in prostitutes from third countries are also linked to trafficking in forged identity papers, drugs, etc.) and conventional criminal organisations are increasingly making use of new technologies to further their aims.

The activities of criminal networks are no longer confined within borders and such organisations are increasingly operating in a number of different countries: owing to the Internet's decentralised structure, relatively complex situations can exist in which an organisation can reach victims living in several different countries and/or have members living in several different countries.

The existence of mobile telephony via satellite provides an additional opportunity for criminal organisations to operate across borders.

'Cybercrime' has a number of specific features:

- the technologies used are constantly evolving;
- finding evidence is an extremely complex task;
- the evidence itself is volatile and modifiable, and is thus easy to tamper with;
- investigators need to be highly skilled.

Such specific characteristics make it necessary for the police and judicial authorities responsible for combating these types of crime to learn new skills, and for cooperation to become more systematic between magistrates and police forces in the various countries.

## **2 EXISTING ADMINISTRATIVE STRUCTURES**

### **2.1 WITHIN THE MEMBER STATES**

#### **2.1.1 Different approaches**

The roles played by the Ministries of Justice and Home Affairs, the Public Prosecutor's Office, the judiciary and the police vary from country to country within the European Union. Although the roles played by the above ministries and the Public Prosecutor's Office are much the same in all countries, there can be major differences in criminal investigation procedures. Unlike in southern European countries, there are no investigating magistrates in northern countries, where

criminal enquiries are carried out by the police and the judiciary's role is confined to the courts, after the accused has been charged.

### **2.1.2 In some countries, there are a large number of different bodies**

There are two broad categories:

- bodies responsible for preventive and regulatory activities (preparation of changes to criminal law and regulations, the drawing up of international conventions on mutual assistance in enforcement activities, etc.);
- enforcement agencies: police services and prosecution services, which are responsible for criminal investigations, and the courts, whose job it is to try the accused.

In general, therefore, in all countries combating organised crime is the job of two principal agencies: the Justice and Home Affairs Ministries and the judicial authorities (the courts).

Specialised departments generally exist within the above bodies, to deal with each category of crime.

In France, each specialised service is responsible for investigating common law offences committed on the Internet in its specific area (e.g. procuring, paedophilia, etc.) and has trained police officers among its officials, who are capable of carrying out investigations on the network. The same applies to the Customs Service and the Gendarmerie.

When one takes both operational and administrative services into account, certain countries may be said to have a particularly large number of bodies involved in combating organised and other types of crime. A list of the relevant bodies in France is given below, by way of an example.

This situation can cause confusion and make it difficult to find the right person to talk to and to exchange information effectively; it can also hamper efforts to cross-reference information on complex cases.

Some national parliamentary reports have drawn attention to the fact that this type of organisation is ill-equipped to respond to the needs of an international set-up with a wide range of diplomatic, technical and procedural implications (cf. the Alex Turk report, in France).

In some countries, such as France, new structures have been set up with a view to improving coordination of enforcement activities. For example, in mid-1998, a 'central unit for the coordination of new information technologies' was set up inside the Central Directorate for Criminal Investigations, with a view to implementing the recommendations put forward by the G8.

## **Excessively complicated structures - the situation in France**

- Services reporting to the Prime Minister
  - Directorate for Information System Security: puts forward policy proposals and monitors implementation;
  - Central Information System Security Service (SCSSI): responsible for cryptology, protection against harmful parasitic signals, and computer security
- Foreign Ministry
  - Sub-Directorate for Internal Community Affairs
  - Sub-Directorate for International Economic Law and Community Law
  - Aliens Department
  - Sub-Directorate for Security, which has horizontal responsibility for terrorism, drugs and organised crime, and is responsible for network consistency
- Justice Ministry
  - European and International Criminal Law Office, responsible for conventions on mutual assistance in enforcement activities
  - Directorate for Criminal Prosecutions and Pardons
- Ministry for Economic and Financial Affairs and Industry (Directorate-General for Customs and Indirect **Taxes**)
  - Sub-Directorate for the Organisation of Surveillance and Resources, which deals with technical aspects of telecommunications
  - Fraud Office
- Defence Ministry (Directorate-General for the Gendarmerie)
  - Office for European Police Cooperation and Legal Affairs
- Interior Ministry
  - Directorate for Civil Liberties and Legal Affairs
  - Central Directorate for Criminal Investigations
    - International Relations Division
    - Sub-Directorate for Criminal Affairs:
      - Organised crime analysis section
        - crime unit
        - trafficking in human beings unit
        - crimes against property unit
        - trafficking in firearms and biological and chemical substances unit

- drugs trafficking unit
  - large-scale financial crime unit
  - counterfeit money unit
- IT fraud investigation service
- Computer crime brigade
- Sub-Directorate for technical and forensic police services  
**(responsible for the management of large applications and running the central NIT coordination unit)**
- Central Directorate for immigration controls and combating the employment of illegal immigrants
  - International technical police cooperation service
  - Anti-drugs mission
  - Anti-terrorism coordination unit
  - Transmissions and data-processing directorate  
**(technical management of databases and access)**
  - Intelligence Directorate
  - Judicial authorities
  - courts

In Italy, the way in which the judiciary is organised has recently been changed. The Public Prosecutor's Office now has complete control over the judicial investigation and cases are no longer passed on to investigating magistrates, as is the case in France or Belgium.

### **2.1.3 Involvement in supranational mutual assistance structures**

Any one country can belong to several different regional or international bodies. These 'cooperation networks' can broaden a country's range of contacts, but problems can arise owing to different working methods or the use of different tools. On the other hand, convergence is possible if the national representatives are the same in all the various supranational bodies.

Some European countries belong to all of the following international bodies:

- Interpol
- the G8
- the Council of Europe
- the European Union



## **2.2 AT INTERNATIONAL LEVEL**

By way of reminder, a round-up of the supranational bodies (other than the EU) in which EU Member States are involved is given below.

### **2.2.1 Interpol**

One of the missions assigned to ICPO-Interpol is to ensure permanent, swift, reliable and secure data exchange between Member States. The first three conditions are dependent on the telecommunications network, while the fourth is dependent on encryption systems.

In 1991 Interpol chose the international **X.400** standard for its electronic mail service because it presented the following advantages:

- compatibility with a wide range of hardware systems;
- different types of terminals can be connected;
- cheap upgrades in the event of changes to the standard;
- value-added services, such as data and image transmission.

The National Central Bureaux (NCBs) were therefore encouraged to acquire e-mail servers complying with this standard; this has now been done in most European countries. **An X.25** communication protocol is used (also used by airlines, among others). ISDN access is possible.

The encryption system used is suited to all types of microcomputer and enables communications to be encrypted end-to-end and for the sender to be authenticated by means of a smart card-based electronic signature.

The ASF system is a data communication system which enables Interpol NCBs and official police services to carry out searches on the database located at the general secretariat (suspects' identities, photos, fingerprints, multilingual datasheets, etc.). Searches can be based on phonetic symbols.

The criminal information system (CIS) contains several files (names of people implicated in international offences, drug seizures, counterfeit money seizures, thefts of works of art, etc.). It also contains personal data sheets and notices of stolen or wanted goods, as well as special notices describing the 'modi operandi' used by international criminals.

Training courses are available for police officers.

**An** Interpol European working party on computer crime has been set up.

### **2.2.2 The G8**

Following the **G8** Summit in Denver, a meeting of Justice and Home Affairs Ministers was held on 9 and 10 December 1997 with a view to stepping up efforts to implement the **40** recommendations on more effective action against organised crime, set out at the Lyons summit. Ten principles and a ten-point action plan were adopted.

Explicit mention was made therein of the use of video-conferencing as a means of taking statements from witnesses located in other countries. Coordination units are currently being set up in each of the eight countries.

### **2.2.3 The Council of Europe**

Several years ago, the Council of Europe set up a European Committee on Legal Cooperation (CDCJ), which itself set up a committee of experts on the processing of legislative and judicial data (CJ-LJ). The 13th seminar on legal data-processing in Europe, held in Vienna from 15 to 17 April 1998, provided an opportunity to take stock of the use of information technology in the legal systems of several countries (principally for document processing purposes).

## **2.3 WITHIN THE EUROPEAN UNION**

Over the past few years several measures and joint actions have been adopted in both the police cooperation and judicial cooperation fields with a view to combating crime (pursuant to Article K.3 of the Treaty on European Union).

Furthermore, several working parties have been set up under the third pillar, including a multidisciplinary group on organised crime.

### **2.3.1 Police and customs cooperation**

#### **Police cooperation**

Police cooperation has been going on for a long time, and policemen are used to travelling around and exchanging information either bilaterally or through Interpol. At European level, the European Information System (EIS), which is based on the Schengen Information System, is a prime example of successful cooperation using a shared tool, which is now operational.

#### **Customs cooperation**

Customs cooperation is included in this study because various types of organised fraud (such as in the financial field) can be detected by customs services.

The computer network used by customs services is currently being assessed for STOA by Mr Maurizio Pedrelli (EP/IV/B/STOA/98/C04.01). We would refer readers to that document for more detailed information. For almost ten years now the integration of the computer systems of the EU's customs services has been based on programmes focusing on information technology (which since 1997 have been brought together under Customs 2000 and Fiscalis). Several computer applications have been introduced at European level to facilitate exchanges of information on VAT and goods transit, the follow-up of sensitive goods, and to manage data on tariffs.

Two applications have been developed with a view to combating fraud:

- **AFIS** (Anti-Fraud Information System), which links national administrations to the Commission and serves as a basis for other applications (such as CIS, EWS, etc.);
- **SCENT** (Secure Customs Enforcement Network), which is a system for the exchange of messages between the Commission and the Member States.

400 terminals are connected to the above applications.

DG XXI assisted in the development of a dedicated communication system for the customs services of all Member States, known as CCN/CSI (Common Communication Network for file transfer and interactive data exchange/Common System Interface). This system should be brought into operation in mid-1999 and will incorporate the initial applications referred to above. It will ensure that data are made secure, so as to prevent third parties from gaining access to them.

## **Europol**

The main purpose of Europol, which was set up in 1995, is to foster the exchange of information between EU Member States. It comes under intergovernmental cooperation arrangements and, for the moment, has no operational powers (its job being to facilitate investigations in the Member States). It has clearly defined powers of intervention (only in the case of serious crimes committed by criminal organisations operating in at least two countries). There are one or more liaison officers (ELOs) in each country.

Europol manages a computerised information system into which data is fed by the Member States and which uses a special data protection system. A call for tenders will be published in 1999 for the supply of the network which is to link up the various national centres.

For the moment, the Europol Drugs Unit (EDU) is the only body which can maintain a comprehensive database indicating the data entered and the names of the persons involved. Once the Europol agreements come into force throughout Europe (which should happen during 1999), it will be possible for central databases to be set up and for information forwarded by any of the national units to be made available to all the other countries.

**Relations with Europol are to be formalised three years after the setting up of the European Judicial Network so as to make it possible for use to be made of the infrastructure which has been set in place.**

### **2.3.2 Cross-border judicial cooperation**

Unlike police cooperation, judicial cooperation is a new development at EU level (if one disregards cooperation between two or three neighbouring countries under bilateral conventions or agreements).

Closer cooperation, particularly in criminal matters, is now universally thought to be essential. The main objective of the work being undertaken in the field of judicial cooperation in criminal matters is to establish a legal framework enabling investigators and magistrates from various Member States to cooperate in following up 'transnational' criminal cases.

Those involved in the administration of justice have high hopes of the measures currently being introduced, but many of the people spoken to feel that a practical, step-by-step approach to the establishment of the 'European Judicial Network' is required.

At the end of **1999**, an important meeting will be held in the framework of the European Grotius programme in order to evaluate the progress made in judicial cooperation and to define what the next stages should be.

### **The European Judicial Network**

On **29 June 1998**, with a view to stepping up judicial cooperation between the Member States *in* combating organised crime and, in the long run, placing judicial cooperation on the same level as police cooperation, the Council adopted a joint action establishing a structure called the 'European Judicial Network'.

The principles governing the organisation and operation of this network are set out in the text published in the Official Journal of the European Communities of **7 July 1998**.

The network comprises a number of 'judicial contact points', i.e. intermediaries whose job it is to exchange information by various technical means, meet periodically and draw up documents or develop tools to facilitate cooperation between Member States.

The network comes directly under the Council Secretariat.

#### Contact points

Unlike in the police cooperation network, where a central contact point was appointed for each country (for example, the Interpol NCBs), in the judicial cooperation network, several contact points are appointed in each EU Member State, **so** as to speed up exchanges of information.

The way in which contact points are selected varies greatly from country to country, owing to the different constitutional rules, legal traditions and internal structures in each:

- 1 per Land (**16** contact points in all) in Germany, with the same in Austria (**1** at each Oberlandesgericht);
- 25** in Italy (**24** public prosecutors at the Public Prosecutor's Office and the chief magistrate of the judicial mutual assistance and cooperation office of the Justice Ministry);
- 3** in Finland (Justice Ministry, Public Prosecutor's Office, police force);
- 2** in France (within the Justice Ministry), backed up by a national network of contact points (1 for each of the **33** Public Prosecutor's Offices);
- 1 in Greece;
- 1 in Ireland, backed up by a network of agencies pledged to provide mutual assistance;
- etc.

Three plenary meetings of contact points are to be held each year (the first was held on **25 September 1998** and the second, on **27 January 1999**). These meetings are used to discuss practical and legal problems arising in the field of judicial cooperation, together with the development of common tools.

The network is gradually becoming established but contacts and meetings remain limited in scope. Not all the contact points are present at international meetings. It will take time for the contact points to get to know each other and to contact each other directly. Moreover, the information to be disseminated through the network is still limited.

## Common tools

The following tools are currently being developed pursuant to the joint action:

- a list of contact points in each country, together with full details on how they may be contacted (telephone and fax numbers), the languages spoken by each contact point and when they may be contacted outside office hours;
- a directory of local authorities;
- concise legal and practical details regarding the legal and procedural systems used in each of the 15 Member States, in the form of standardised data sheets, known as 'Belgian data sheets';
- a compendium of agreements, declarations and reservations.

The above information, part of which is confidential, will be made available to all magistrates in charge of cases involving organised crime.

## Technical resources

The joint action provides for the use of a telecommunications network on which data may be made available and which may be used by contact points to exchange information.

In late 1998 it was decided to use CD-ROMS as a provisional means of sharing the four types of tool referred to above, once they are ready. The CD-ROM should be ready for a meeting to be held in June 1999. **The use of a 'secure' telecommunications network was judged premature, since for the moment it would be too costly and too much of a handicap for those contact points which do not yet have the necessary equipment.**

However, as was mentioned earlier, relations with Europol are to be formalised three years after the setting up of the European Judicial Network, so as to make it possible for use to be made of the infrastructure which has been set in place.

## **3 EQUIPMENT AND TECHNICAL INFRASTRUCTURE**

### **3.1 THE BENEFITS OF NEW TECHNOLOGIES**

The term new technologies covers both computer and data-processing technologies and remote communication and data transfer technologies.

#### **3.1.1 The benefits of computer technology**

The main advantages are generally considered to be:

- less time spent by staff on processing data;
- data needs to be re-entered less frequently;
- data can be forwarded more quickly, when systems are linked up to telecommunications tools;
- management data are generated as a by-product of operational activities.

Computer technology can be used at various stages in the judicial process:

- administrative follow-up of criminal proceedings

This involves the recording of administrative data on each case **so** that any magistrate can ascertain the stage reached in the proceedings, the purpose of those proceedings, who is involved, and **so** on.

All data recorded at a given stage in the proceedings can be accessed at a later stage, without the need for data to be re-encoded or re-entered.

- personal data

Data on anyone with a criminal involvement in a case needs to be readily accessible (information on people implicated in current cases, criminal records, the identity of vehicle owners, etc.).

- documents connected with cases

The use of computer technology can be restricted simply to lists of documents connected with cases. This can save magistrates a lot of time when they are dealing with extremely bulky files and need to be able to find a document quickly during the course of proceedings.

However, the contents of documents can also be digitised. This presents the advantage of being able to leave the original documents in the file, while enabling them to be consulted simultaneously by several different people. At the same time, through the use of certain types of software (text analysers), it enables cross-references to be established between data either inside a given file (names or events referred to by several witnesses or in several investigator's reports, etc.) or between several different cases. This type of procedure is referred to as 'electronic document management' or 'computer-assisted investigation', and systems of this kind already exist in several European countries.

- drafting of international judicial assistance documents (such as letters rogatory)

Given that laws, agreements and practices vary greatly from country to country, computer and artificial intelligence technologies can provide useful assistance in ensuring that judicial assistance and other requests forwarded to another country are properly formulated. (**An** expert system of this kind has been developed by the Justice Ministry in the Netherlands.)

- translation

In view of the EU's linguistic diversity, computer-assisted translation tools can prove useful and can, of course, be used in tandem with the other tools referred to above.

Given the potential benefits, the use of computer technology is steadily becoming more widespread in the legal systems of the various Member States.

Other types of application can also be of use to magistrates or administrative departments:

- access to legal documentation

Databases can be used to store large numbers of legal texts, ranging from national and European legislation and regulations, case law and legal literature to the substance of agreements and

conventions concluded between countries. Many other types of documentary resource can also be processed electronically.

- statistics and flow management

Judicial assistance requests can enter some countries through various different channels, which means that it is not always possible to keep track of the flow of such requests or the time taken to act on them. Although direct contacts are productive, they do not enable the people concerned to gain an overall picture of the situation and to establish cross-references between interdependent cases, whence the advantage of having a national system for the recording of incoming judicial requests (possibly going beyond mere letters rogatory).

### **3.1.2 The benefits of telecommunication technologies**

Fixed telephones have been in widespread use for many years and mobile telephones now allow people to get in touch with others or to be contacted wherever they are.

Photocopiers are now almost universally used for professional purposes, for the real-time transfer of text and images.

Electronic mail (e-mail) can be used to exchange text, photographs, sound recordings and so on (as long as they have been digitised) with one or more correspondents and with the added advantage over the fax of the fact that the data received can be reprocessed directly on a computer.

Telecommunications networks also enable people to gain remote access to the type of 'data sources' mentioned above, namely files (whether central or not) compiled by various bodies (such as criminal records), legal databases, electronic case files, and so on. The only precondition is that the data must have been digitised and stored in a system connected up to a telecommunications network.

#### Video-conferencing

**A** seminar on the prospects for the use of video-conferencing in criminal proceedings in Europe was held in Paris on 27 November 1998. Several speakers emphasised the considerable benefits brought by video-conferencing in the field of judicial mutual assistance and in connection with international letters rogatory, particularly with regard to the examination of witnesses and the remote consultation of experts. **As** we have seen, criminal networks extend over several different countries and witnesses in a given case can therefore be located relatively far away from each other. Using conventional methods, proceedings are time-consuming and it is almost impossible simultaneously to examine witnesses located in different countries and, where appropriate, to bring them 'face-to-face' with one another. One of the advantages of video-conferencing is that it can be used to organise this type of confrontation and to compare the evidence given in real time. It also guards against the possibility of witnesses being intimidated. Lastly, it enables a faithful record to be kept of examinations of witnesses (and for witnesses not present at a trial to be examined, although this should only be done under exceptional circumstances, since witnesses are more convincing if they are physically present). The cost involved, excluding the initial investment, is low compared to the cost of a magistrate actually travelling to the countries in which the witnesses to be examined live.

In the United States all district attorneys' offices now have a video-conference room. There are even plans to use video-technology to provide remote guidance for searches and to indicate where to look.

Video-conferencing can be seen as a step forward, but requires high-quality links (2Mbytes, ATM, etc.), suitable premises and so on, and will therefore not become common practice in the near future. Furthermore, several basic problems need to be solved, such as the examination procedures to be used, the fact that the screen distorts one's perception of objects, and psychological considerations vis-à-vis the witness which need to be taken into account.

### **3.1.3 Identification and authentication devices**

Current techniques enable extended use to be controlled by two basic functions designed to protect access to data transmitted over a network: identification of persons and transaction authentication.

The first function simply involves checking the identity of the individual concerned. Current techniques enable this to be done in a number of ways: entering a confidential password or the recognition of some characteristic recorded on a physical medium using a magnetic strip or an embedded chip. In future, it will be possible to make use of other distinguishing characteristics, for example, finger prints.

Authentication consists of guaranteeing the origin of a transaction (or a document) by adding identification data to the data that make up the transaction itself.

Whatever technique is used, identification enables diversified applications to be 'piloted':

- access authorisation (to a computer, one's own files on a server, specific shared electronic files, specific databases, but also the right of access to one's office, specific parts of a building, or a car park, etc.);
- authentication of an act carried out by an operator: this is partly related to the issue of electronic signatures, which is currently being looked into by the banking sector and also as part of the European project EUROLOOK;
- everything relating to 'electronic money' and transactions involving financial flows.

Identification devices are essential in order to introduce a 'paperless' system based on electronic media and to reduce the amount of time taken to carry out certain operations. But a technical solution must be found that is both simple to use, and above all reliable, and which also provides protection against the possibility of fraud or breach of trust.

## **3.2 THE CURRENT SITUATION IN THE MEMBER STATES**

### **3.2.1 Overview**

The degree of use of new information and communication technologies (such as microcomputers, electronic mail, Internet files, video-conferencing, etc.) varies greatly from Member State to Member State and, inside each Member State from body to body.



Some of the computer systems which exist were built several years ago and are based on 'closed' technology which hampers migration to more modern technologies, integration into larger systems (within a given service, or between several services) and interconnection.

To date, each separate judicial body has tended to develop its own systems and protocols. In some cases, surveys have shown that systems do not fully meet their users' needs (in terms of user-friendliness, data reliability, data retrieval criteria, etc.).

### **3.2.2 A few examples**

#### France:

- The European Judicial Network correspondents in the 33 Public Prosecutor's Offices are to be equipped with a fax and a portable telephone in the near future.
- Justice Ministry: officials still have only limited access to computer tools and remote documentary resources. **An** intranet is currently being set up with a view to linking up each court (and, in the long run, each magistrate) via the e-mail service and, subsequently, to link up all the various criminal justice databases. The Foreign Ministry is also in the process **of** developing an intranet and digitising all documents connected with measures to combat organised crime, with a view to improving coordination between departments.
- The courts: there have been numerous delays and problems in the process of **computensig** French courts. With the exception of courts in the Paris region, in which what is **known** as the 'nouvelle chaîne pénale' (a case follow-up application) managed by the Chancery has been introduced, computer systems have been decentralised to the appeal courts, on the basis of a 'judicial information technology charter' adopted in September 1994. **The** computerisation of appeal courts and courts of first instance is nearing completion (with an average ratio of two officials per work station) and has generated major productivity gains. However, there is a degree of inconsistency in the hardware and software used, which are often incompatible (hampering data exchange and making it harder for staff to adjust when they are transferred). There are also problems regarding the training of officials, which is not always adequate, hardware maintenance, dependence on a few large computer companies, slow technical support and cumbersome budgetary procedures covering current expenditure.

**Furthermore, few magistrates have direct access to legal documentation databases (legislation and case law).**

In the courts, only very few magistrates can gain access to computerised files by means of electronic document management systems or 'computer-assisted investigation' systems (at the moment, on stand-alone PCs).

In spite of widespread reticence owing to the fact that telecommunications systems are not secure, the number of magistrates with an e-mail address is growing daily at all levels of the hierarchy, and extensive use is made of e-mail to exchange information, not least with magistrates in other countries. Some magistrates have joined 'distribution lists' (such as Jugenet, which brings together 200 French-speaking magistrates in 20 countries, Themis-France, designed to ensure the rapid distribution of professional documents, Law-France, dealing with the practice of law, etc.).

Nonetheless, documents relating to international judicial assistance and cross-border letters rogatory are still forwarded by conventional means.

### Portugal

The use of new technologies in the legal field is based on the programme for the computerisation of the judiciary adopted in 1997, which has three strands:

- the computerisation of courts and the setting up of a national network (access to administrative databases, follow-up of cases, the recording of investigation data, etc.);
- the design and introduction by mid-1999 of an integrated criminal information system for the Criminal Investigation Service;
- the redesign of the legislation and court judgment information system, with a view to enhancing its consistency and making it available on the Internet.

A programme to supply magistrates with microcomputers and provide training in dedicated applications is currently in progress.

### Spain

All magistrates have their own microcomputer, together with access to a special legal databank (CENDOJ); an intranet is currently being installed to link up all courts and magistrates. It would appear that, for the moment, magistrates do **not** have access to the Internet nor do they have e-mail or mobile telephones supplied by the Ministry or the CGPJ (General Council of the Judiciary).

The follow-up of cases is to be computerised in two or three years' time. Computerised files containing supporting evidence sometimes exist for the most important organised crime cases (dealt with by the 'Juzgados Centrales de Instrucción').

Magistrates do not have direct access to files kept by the police. Information is forwarded in hard-copy form.

None of the courts have a video-conference room.

### The Netherlands

A large number of magistrates are equipped with a microcomputer. In 1997 the Office for International Judicial Assistance in Criminal Matters developed an expert system (Kennissysteem Rechtshulpverzoek In Strafzaken) on diskette, which guides magistrates through the maze of agreements and regulations existing in this area, before producing the final documents to be sent abroad (within and outside the EU) - including both letters rogatory and all other forms of requests made under judicial assistance procedures. The final document is printed out in one of four possible languages (English, French, German and Spanish). There are plans to make this system available on CD-ROM in the near future, so that it may be used more widely within the country. (It would need to be adapted for use in another country).

## Finland

All magistrates have a microcomputer fitted with a modem, a fax, a portable telephone and e-mail; the use of these technologies is now common practice.

### **3.3 AT EUROPEAN LEVEL**

#### **3.3.1 Common tools**

A number of tools have been introduced or are in the process of being introduced in the police and judicial spheres:

- The Schengen Information System (SIS), which was introduced in 1996 following the transposition of the Convention applying the Schengen Agreement of 14 June 1985, is intended to improve controls at the EU's external borders by ensuring the rapid dissemination of information on wanted persons and individuals under surveillance. It comprises files containing personal data together with administrative and legal information. It also covers certain types of goods such as works of art.
- The European Judicial Network system

Following the meeting on 'options for a telecommunications network', at which three options were put forward (distribution on CD-ROM, distribution via the Internet, or development of an Intranet), the first of the three options was adopted on a provisional basis by the Council Secretariat's Data-processing Service in November 1998.

National representatives rejected the idea of a dedicated telecommunications network for the EJN, on various grounds, such as the cost of a secure system and the fact that some contact points did not have computers.

Thus ~~far~~, it has not been deemed appropriate for Europol's computer resources to be used, given that Europol has a single contact point per country while the EJN has several.

The decision on whether to move over to an intranet or Internet server has been deferred until 1999-2000.

There is currently no provision for the exchange of operational information (for example, for data security reasons, there are no plans to disseminate evidence).

#### **3.3.2 Data exchange between judicial authorities**

Data may be exchanged between the judicial authorities in the various Member States by various means:

- orally or by means of voice recordings;
- typed documents;
- documents containing graphs, figures and tables;
- images: counterfeit banknotes, fingerprints, photographs;
- combinations of text and images (notices);

- the consultation of databases.

The EDIJustice project (under the European TEDIS programme), which was launched in 1995, is intended to facilitate electronic data exchange. However, there have been no practical spin-offs to date.

The **IDA (Interchange of Data between Administrations) programme**, which is one of the operations being conducted by the Commission (DG III) with a view to preparing for the information society, proposes a pragmatic, coordinated approach to the introduction of pan-European telematic services and the migration of administrative procedures from hard-copy to electronic format. The goal is to help authorities in the various European countries to communicate with each other and to harness best practice in this area.

To date, no initiatives have been taken in the judicial sphere under the above programme. Attention should, however, be drawn to a customs project and the ITCG project on trafficking in cultural goods (feasibility study on the interconnection of national databases and the protection of the data contained therein).

#### **4 OBSTACLES STANDING IN THE WAY OF ACTION TO COMBAT CROSS-BORDER ORGANISED CRIME**

A number of obstacles are hampering the effectiveness of judicial cooperation between the Member States:

##### **4.1 Differences in national legislation and practice**

According to the people we spoke to, at the moment the main problem inside the European judicial area is not technological disparities but disparities in national legislation.

The significant differences in legislation (prevention, offences and crimes) and tradition still to be found make the definition of common offences a delicate matter. This also applies to the concept of evidence (given items of evidence are admissible in some countries and not in others).

The way in which the legal system is organised and the roles played by the police and by magistrates also varies from Member State to Member State, as do confidentiality rules (in Finland, **for** example, there is **full** transparency from the moment someone **is** charged). Furthermore, in some countries, letters rogatory may not be forwarded to the Customs Service, and various other barriers still also exist (such as the banking secrecy law in Luxembourg).

Nonetheless, new acts are gradually being adopted to take account of new technologies. At EU level, the Convention on Mutual Legal Assistance in Criminal Matters which is currently being drawn up seeks to solve problems arising in connection with the 'cross-border' collection of evidence and to simplify and speed up proceedings. It should, *inter alia*, make it easier to obtain evidence from other countries, strengthen agreements on investigations and seizures, and enable investigators and magistrates to contact each other directly and exchange information.

Several EU Member States have recently adopted new laws or amending laws to take account of new technologies:

- Italy: Law No 11 of 7 January 1998 authorises remote participation in criminal proceedings via an audiovisual link;
- France: the law of 5 January 1998 (known as the 'Godfrain Law') introduced criminal provisions designed to protect computer systems against conventional and new forms of computer crime.

## **4.2 Cumbersome administrative procedures and lack of legal approval**

Certain formal procedures (notification, etc.) have no place in action to combat crime. Furthermore, what is the point of being able to transfer information in real time if that information is then left 'on hold' for days or weeks in hierarchical or administrative structures?

Attempts to pool resources are often hampered by the fact that not everyone shares the same approach (for instance, some countries make no distinction between what comes under 'intelligence' and what comes under 'crime'); the necessary files exist, but there is no cooperation. The technical arrangements (thesaurus, images, etc.) for interconnecting files on works of art have been set in place, but legal approval is not forthcoming; the same is true of the file on armed robberies, the drugs analysis file (designed by the forensic science laboratory in Lyons) and the genetic fingerprints file.

Major problems have arisen in the current discussions between Member States on the interception of GSM and Internet communications, cryptology and other matters, including authorisation to collect evidence or identification details in another country. Few countries are willing to give up part of their sovereignty. No concrete decisions have therefore been taken to enable operational services to get to work.

## **4.3 Access to legal documentation**

The term 'legal documentation' covers national and European laws and regulations, case law and comparative law studies. Most national and European documentary resources were digitised many years ago (the first database was established in 1970). Much of that documentation is now available on-line via database servers, or on **CD-ROM**. Studies are currently in progress in several countries into how these resources might be made available on the Internet (the first set of documents was placed on the Internet in 1995). Seminars on the processing of legal documentation in Europe are held periodically under the auspices of the Council of Europe. The basic problem is not the accessibility of such documentation, but access costs (in certain countries), disparities in consultation and query tools and, above all, linguistic diversity.

In practice, few magistrates are themselves able to retrieve and use foreign legal documents (language problems, different file organisation methods, tools, etc.). The comparative studies undertaken by the European Judicial Network contract points are therefore of strategic importance.

## **4.4 Linguistic diversity**

The fact that the Member States do not all use the same language constitutes a barrier to the exchange of information, even though people at a given level of responsibility might be expected

to know at least one foreign language. Nonetheless, legislative texts, administrative documents, files and evidence are rarely available in more than one language.

#### **4.5 Data protection**

In most countries, it is illegal to merge files containing personal data compiled by various departments and to forward that data without the consent of the person concerned.

#### **4.6 Lack of access to files**

Various files are compiled in each country by the police and judicial authorities (for example, criminal records). These files are often not available on line even inside a given country, which makes them all the more difficult for magistrates from other countries to gain access to.. In France, for example, the only means available to magistrates wishing to 'consult' the criminal records held in Nantes is by sending a fax to the department responsible.

It might be useful to cross-reference the information held in the various countries (so as to ascertain whether a given person already has a criminal record in another country).

#### **4.7 File incompatibility**

Files compiled by the various police and judicial authorities are not always compatible, even inside a given country. Different bodies use different file structures, which makes consultation difficult, even in cases where it is authorised and appropriate.

Furthermore, most existing files should be gradually transferred to open platforms, but that is a costly process.

#### **4.8 Inadequate staff training**

In order for new technologies to be used effectively, the staff involved in legal cases must have both the necessary processing and communication equipment and the skills required to make the best possible use of these new tools. This requires both training and the simplification of the tools themselves.

In France, for example, young magistrates will have undergone computer training during their studies and have been provided with a microcomputer, but the same cannot be said for all magistrates already in service.

#### **4.9 Territorial limitations**

While judicial cooperation between the 15 EU Member States is an obvious necessity, many of the people spoken to emphasise the need to extend the relevant tools to the EU's neighbours (the Baltic States and the Central European countries).

#### **4.10 Computer evidence**

Over and above the difficulties traditionally encountered in intergovernmental cooperation, a number of specific problems arise in connection with 'cybercrime', including: the monitoring by investigators by electronic communications; collecting evidence of computer crime (major disparities at national level regarding the collection and admissibility of evidence); the conduct

of cross-border searches; halting the transmission of messages with an illegal content; and the coordination of legal proceedings. The development of **GSM** satellite communication systems will make interception even more difficult.

The International Organisation on Computer Evidence (OIPRO/IOCE), which was set **up** in **1993**, has **45** member organisations representing 25 countries. It recently tackled the growing problem of crimes committed on the Internet. Working parties have now been set up to draw up standards **for** computer evidence (the results of work on terminology were submitted in October **1998**). **A** link has been established with the European Network of Forensic Science Institutes (ENSFI) with a view to the examination of these standards.

The data we are concerned with here are volatile and can be modified (messages are not always saved on the hard disc of the access provider or the criminal); precautions must also be taken to ensure that the data which is stored cannot be modified subsequently (whether accidentally or with illicit intent).

## **5 COMMUNITY ACTION**

### **5.1 Comparison of legislation and practice**

- Within the European Judicial Network

Major efforts are being made to facilitate the cross-border collection of information. The plenary meeting adopted a list of 32 survey measures and for each measure a 'standard data sheet' containing **10** to **20** headings will be drawn up, listing the criminal procedures in each of the **15** Member States. **A** terminological survey will also be conducted.

In terms of volume, for each of the **15** Member States there will be:

- one page on the organisation of the judicial system (who does what in each country; the basic roles played by each of the people involved in a case);
- **150** data sheets describing legal procedures and practices.

All the above data will be available initially in French and in English, and subsequently also in German.

- Rules on money-laundering

In another context, similar work is being undertaken on national rules and practice regarding money-laundering. This involves a three-member committee studying and assessing the situation in a country which is not their own and then drawing up a report for the other countries.

- Documents on computer crime

On 29 September 1998 a list of documents was published further to the report on work conducted at international level to combat the criminal use of new technologies (Crimorg 44, March 1998). This list contains the documents published by the European Union, the Council of Europe, G8 and the OECD (ICCP), classified by subject area.

## 5.2 Data protection

As part of the European IDA programme, a number of important documents have been drawn up on the issues of the validity of data exchanged, data protection, user rights and duties, and security. These include a data protection guide and a document on legal issues connected with data exchanges between administrations. A link has been established with some of the projects being conducted under the European TEDIS II programme.

## 5.3 Training

- the Falcone programme

The Falcone programme, which was adopted on 19 March 1998, is a multiannual programme (1998-2002) of exchanges, training and cooperation for persons responsible for action to combat organised crime. It seeks to remove barriers to cooperation between the Member States by setting various specific objectives such as improving professional expertise and familiarity with current legislation and procedures, and organising joint projects (comparability and circulation of information, training, studies, improving operational methods).

Other programmes:

- the Grotius programme, which seeks to facilitate judicial cooperation by enhancing familiarity with the procedures and judicial institutions of the various Member States, and by promoting exchanges of experience and the establishment of work contacts;
- the Oisín programme, which seeks to improve cooperation between enforcement agencies in the Member States, to enhance familiarity with legal systems and enforcement practices, and to raise the level of the expertise of staff working in the relevant departments;
- the Stop programme, which seeks to strengthen cooperation networks in the field of action to combat trafficking in human beings and the sexual exploitation of children;
- the Sherlock programme, which seeks to improve the effectiveness of action to combat the production of counterfeit identity papers and other documents.



## **6 A VISION OF THE FUTURE OF JUDICIAL COOPERATION**

### **6.1 POLICE AND JUDICIAL COOPERATION ACTORS**

#### **6.1.1 Police cooperation**

Police cooperation at national and international level consists of the exchange of information and assistance relating to the search for, identification, filing information on and monitoring of criminals.

Cooperation may be occasional or organised systematically (for example within the framework of the Schengen agreements), and may be bilateral or multilateral.

#### **6.1.2 Judicial cooperation**

Crimes and offences are only dealt with by the judicial authorities once they have been notified to the Public Prosecutor's Office.

The public prosecutor and/or the investigating magistrate oversee the judicial investigation or the inquiry by, among other things, assigning 'investigative duties' to the police.

At international level, the Public Prosecutor's Office and the investigating magistrate of the country of origin (applicant) submit these duties to the judicial or administrative authorities of the recipient state (requested state), with a view to their being carried out by the state in question.

The authorities also cooperate on the implementation of hundreds of judicial decisions.

### **6.2 LEVELS AND INSTRUMENTS OF JUDICIAL COOPERATION**

#### **6.2.1 Harmonisation**

International judicial cooperation takes place in accordance with the treaties signed by the states, taking account of the specific political, administrative and judicial characteristics of each state.

These specific characteristics and the resulting differences between national systems make it necessary for all letters rogatory to be processed by the judicial hierarchies in both the applicant and the requested state, which is slow and inefficient.

There would be few problems in setting up an effective system of judicial cooperation if the structures of and relations between the judicial authorities and the police, criminal law, and judicial procedures and practices were identical throughout the Community.

In the long term it will therefore be necessary to move towards harmonisation, while at the same time taking care not to attempt to resolve problems by forcing the pace of any harmonisation. The differences between Member States in terms of structure, the way in which the judiciary and the police interact and judicial procedure and practice mean that, if cooperation is to be successful in the short and medium term, other arrangements will be required.

## **6.2.2 Knowledge of structures and practices in other Union countries and targeted judicial action**

In order to prevent judicial action from being hampered by the current system's serious shortcomings in terms of efficiency and speed, improved knowledge of the judicial structures and procedures of all Union countries is essential.

The standardised information sheets on practices in the area of basic judicial measures in EU countries, which will be distributed on CD-ROM in June 1999 by the General Secretariat of the European Union, will improve knowledge of basic judicial measures and may be supplemented on regular basis so as to provide increasingly exhaustive, precise and up-to-date information.

Over the medium term, a European expert system should also be set up, similar to that introduced in the Netherlands for letters rogatory to be sent abroad. Under such a system, guidance may be given to each Union country to enable it to draw up, in one of the agreed languages, and issue, letters rogatory intended not only for direct recipients in other Union countries but for countries throughout the world.

## **6.2.3 Databases containing information on criminals and criminal organisations**

When an individual, who may or may not belong to an international criminal organisation, is suspected, accused or convicted of a serious crime or offence, the judicial authorities of the country concerned must be able to consult databases, some of which should cover the territory of the European Union, including:

- a national register for each country so that the identity of an individual can be checked (first and second names, date and place of birth, gender, nationality, domicile, etc.);
- a national criminal records database for each country for checking whether an individual has ever been convicted of a crime by the judicial authorities of the country in question;
- a central database for current legal cases to make it possible to find out whether, and in respect of what facts and with what accomplices, an individual is or may be implicated in another case at international level in the European Union, in order to examine the possibility of connections between cases and of the joinder of the new investigation inquiry.

The other information which must be checked such as the use of false names, finger prints, whether or not an individual belongs to an international criminal organisation, connected individuals, whether or not the individual is being detained, etc., is held in police or **prison** databases which have to **be** consulted by the police at the request of the judicial authorities.

## **6.3 JUDICIAL COOPERATION TOOLS**

Harmonisation requires an arsenal of legal and regulatory measures which will take a long time to implement.

Information about judicial structures and practices can be distributed using an unprotected CD-ROM, provided that the information is in the public domain and that no special software is required to consult it.

In view of this, it is curious that the officials of the General Secretariat of the European Union should be so secretive about the EJN contact points when they intend to publish the names, telephone numbers and addresses of the individuals concerned, together with information on

judicial practices, in a non-encrypted form, on a CD-ROM of which anyone could make an exact copy on CD using equipment that can be purchased for EUR 300.

One basic precaution which can be taken to protect sensitive information on a **CD-ROM** would be to encrypt the information recorded on it and to give the decryption key only to the person responsible for using the information.

Information concerning judicial measures is constantly changing since not only is it subject to modification but it also needs to be supplemented, clarified and made more specific.

**A** record in a relational database is therefore a very effective way of keeping the information available up to date.

**A** CD-ROM could be produced periodically to give a complete picture of all the information at a particular point in the year. But the most up-to-date version of the information could be made permanently available over an Intranet.

This would simply involve putting an Internet server on an existing Intranet network belonging to a European body such as Europol. The tools needed to ensure the security and protection of information distributed in this way already exist.

The documents relating to letters rogatory produced using an expert system should be **distributed** by e-mail on a European Intranet network rather than printed on paper, sent by fax and/or **post**

**A** database for important current legal cases in all EU countries would require the **use** of a protected system operated over an Intranet, since a database of this sort has to be updated on a daily basis in order to ensure that the latest information on cases is available.

#### **6.4 THE STRUCTURE OF JUDICIAL COOPERATION**

The prosecution in EU countries, at the level which is of interest to **us**, consists of Public Prosecutor's Offices of First Instance and a number of Principle Public Prosecutor's Offices

Even the level of Principle Public Prosecutor's Office appears ill-equipped to combat cross-border organised crime and a single National Public Prosecutor's Office for each country would seem to offer a more effective solution.

The differences between the Member States in terms of surface area, administrative structure, population and the density of their judicial network are such that there would be wide variations in the size of the National Public Prosecutor's Offices, but their existence would ensure a degree of uniformity in criminal law, judicial procedures and practices, language(s) and relations with the police authorities.

The National Public Prosecutor's Offices could be linked up by Intranet (as discussed above) and have access to appropriate national databases.

They would be the contact points for the other National Public Prosecutor's Offices in the European Union.

They would exchange information on current cases involving international criminals in their respective countries with a Principle Public Prosecutor's Office at European level to which they would submit proposals for joining certain ongoing cases, covering more than one country, because of the connections between them.

The National Public Prosecutor's Offices would also work very closely with their country's Europol representatives and through the Europol network with the police services of the other Member States.

## **Annexes**

**ACC 876**  
**April 1999**  
**Author: Mr Eric Sutter**

## **PEOPLE INTERVIEWED**

### - At European level

- Europol: Mr Willy Bruggeman, Mr David Valls-Russell, Mr Bram Dekker
- EU Council Secretariat: Mr Hans G. Nilson (DG H - Judicial Cooperation) and Mr Johan Vlogaert

### - Belgium

Justice Ministry: Mr C. Debrulle, Mr D. Flore and Mr S. de Biolley

### - Spain

Consejo General del Poder Judicial: Mr Rubén **A.** Jimenez Fernández

### - Italy

Permanent Delegation to the EU: Lorenzo Salazar, delegated magistrate

### - Finland

Justice Ministry: Mr Hannu Taimisto  
Public Prosecutor's Office: Ms Raija Toiviainen

### - France

Foreign Ministry: Mr L. Paillard

Justice Ministry: Mrs Pelsez

Paris Court of First Instance:

- Investigating magistrate: Mr J-P Zanoto
- Deputy Public Prosecutor: Mr David Peyron

Interior Ministry:

- Central NIT Coordination Unit: Mr M. Desfarges
- **Ecole** de la Magistrature (Magistrates Training School), Bordeaux: Mr Coste, Deputy Director

### - Netherlands

Justice Ministry: Mr H.F. Knaapen

## DOCUMENTS CONSULTED

- **European or international documents**

- Proposal for a Council Decision on a **joint action establishing a programme of exchanges, training and cooperation for persons responsible for action to combat organised crime (Falcone programme)**, October 1997 (COM(97)528 final)
- Report on the **proposal for a joint action to create a European judicial network**. Rapporteur: Mr R. Bontempi; 6 November 1997
- Report on **judicial cooperation in criminal matters in the European Union**. Rapporteur: Mr R. Bontempi, 11 February 1998
- European Union **Convention on mutual legal assistance** (draft)
- **Communiqué published by the G8 Justice and Home Affairs Ministers** following their meeting of 9 and 10 December 1997
- **1997 EU Situation Report on Organised Crime**. Report to the European Parliament
- **COMCRJME study** by Professor Sieber, 1998 (on the situation as regards substantive and procedural criminal law in the EU Member States)
- **Joint action of 29 June 1998 on the creation of a European Judicial Network** (98/428/JHA), OJ L 191, 7.7.1998, p. 4
- Council of the European Union: **European Judicial Network: Options for a telecommunications network**, July 1998
- European Commission: **A framework for action on combating fraud and counterfeiting of non-cash means of payment, July 1998** (COM(98)395 final)
- European Commission: **Towards an Area of Freedom, Security and Justice, July 1998** (COM(98)459 final)
- Council of the European Union: **first meeting of European Judicial Network contact points**, 25 September 1998
- **Avignon Declaration** adopted following the seminar on *The European Judicial Area*, 16 October 1998
- Seminar on '**prospects for the use of video-conferencing in criminal proceedings in Europe**', Université Paris IX Dauphine, 27 November 1998
- *Bulletin sur la criminalité technologique*, September 1998



- **State of play of the interstate customs computer network.** Interim study. European Parliament, STOA, December 1998
- **Report on the draft joint action on police cooperation in the EU on the verge of the adoption of standards for joint operations** (14061/98 – C4-0047/99 – 99/0908 (CNS)), **on the draft joint action with regard to combating international crime with fuller cover of the routes used** (14060/98 – C4-0048/99 – 99/0907 (CNS))
- **'Freedom, security and justice: an agenda for Europe'**, interparliamentary conference, Brussels, 24 and 25 March 1999
- **National documents**

#### France

Senate: Information report 49 (96-97), **'Quels moyens pour quelle justice?'** - Committee on Legal Affairs. Rapporteurs: Charles Jolibois and Pierre Fauchon

Senate: Information report **523** (97-98), **'Quand les policiers succèdent aux diplomates'** - Committee on Legal Affairs. Rapporteur: Alex Turk

Council of State: **'Internet et les réseaux numériques'**. Rapporteur: Isabelle Falque-Pierrotin. Adopted on 2 July 1998

#### **Law No. 11 of 7 January 1998**

#### **Excerpts from the Italian Code of Criminal Procedure**

#### **The organisation of the Italian Justice Ministry**

#### Portugal

**New developments in legal data-processing.** Report of the Portuguese delegation, Strasbourg, 4-6 November 1998 (Council of Europe/CJ-IJ 98/16)

**STOA PROGRAMME**  
**European Parliament**  
**Directorate-General for Research**  
**Directorate A**

**Room SCH 04 A034, Schuman Building,  
Kirchberg  
L-2929 Luxembourg,  
Tel (352) 4300.22511;  
Fax (352) 4300.22418 or 24167  
E-mail: rholdsworth@europarl.eu.int**

**Room ASP6D46, Altiero Spinelli Building,  
60, rue Wiertz  
B-1047 Brussels,  
Tel (32-2) 284.3962  
Fax (32-2) 284.9059**