EUROPEAN UNION
THE COUNCIL

Brussels, 13 November 1995 (24.01)
(OR.es)

4354/2/95

REV 2
LIMITE

ENFOPOL 15

N O T E

from: Spanish delegation

to : Technical and Forensic Police Working Party

Nos prev. docs: 4354/1/95 ENFOPOL 15 REV 1 and 8847/95 ENFOPOL 77 + COR 1

Subject: Report on national law in connection with the questionnaire on telephone interception

REPORT ON NATIONAL LAW IN CONNECTION WITH THE QUESTIONNAIRE ON TELEPHONE INTERCEPTION

INTRODUCTION

The definitive text of the abovementioned questionnaire, having been approved by all the delegations present at the meeting in June 1993, was sent to all the Trevi Group countries on 27 July 1993, following instructions from the Chairman of the group of experts.

After replies to the questionnaire had been received from Germany, Denmark, Spain, France, the Netherlands, the United Kingdom, Ireland, Italy and Portugal, a report was drawn up in French, which was submitted to the Group at the meeting held in December 1993. This report was not studied, as it still had to be completed with further additional replies from several delegations, which had been requested on 9 December 1993.

At the Presidency's suggestion, an English translation of this report was sent to all delegations on 23 December 1993 for information and for comments and suggestions.

A new version included both the additional replies received and the comments made (December 1993 – January 1994). On 4 March 1994 the final text was distributed as 5355/94 ENFOPOL 31 for discussion at the Group's meeting on 7 March 1994. After presentation, further oral comments were made. The comments made at the meeting by Ireland and Italy were submitted in writing. At the September 1994 meeting it was agreed

at the Presidency's prompting and pending some additional suggestions, that replies should be included from the new States joining, or about to join, the EU.

The penultimate version took account of the amendments received, the new contributions provided by Austria, Greece, Finland, Norway, Sweden and Luxembourg, and Belgium's contribution.

We wish to thank all delegations who replied to the questionnaire for their collaboration, which made it possible to carry out the assessment of national law needed to attain the aims of our joint work.

At the meeting of the Police Cooperation Working Party on 22 May 1995 it was agreed that the Spanish delegation would update the report. Delegations were therefore given a questionnaire on amendments to national law (8847/95 ENFOPOL 77). This final version includes delegations' replies to the questionnaire for the purpose of updating the report.

A. GENERAL LEGAL SYSTEM

As was to be expected, all the countries which replied to the questionnaire guarantee the confidentiality of private communications under their constitution or constitutional law or in ordinary legislation or in both, in compliance with Article 8 of the European Convention on Human Rights.

Similarly, all countries have legal provisions which permit the practice of telephone interception in particular cases and conditions. In the case of Finland, however, it should be pointed out that the law governing these measures is being amended and, if approved, is expected to enter into force in summer 1995.

In Belgium, procedural law authorizes only the form of interception known as "data control" (detection, counting, metering or pen register) i.e. without access to the contents of the communication. Since a bill to regulate this area of lawful interception is before Parliament, the replies given to the questionnaire by the Belgian delegation reflect this bill.

These legal regulations may be provided for either in codes of criminal procedure only, as happens in Germany, Austria, Denmark, Luxembourg, Spain and Portugal, or in special laws as in Belgium, France, United Kingdom, Ireland, Greece, Norway and Sweden, or in both at the same time, depending on the case in point, as occurs in Italy.

For the moment, interception does not appear to present any legal problem specifically connected with the means of transmission used for transmitting oral, text, data or image communications.

When communications are transmitted through a computer system, the question of

authorized police access is not dealt with in the same way in all the countries.

Germany, Denmark, Spain, Portugal, Austria, Finland, Ireland, Norway and Luxembourg state that such cases are included in the general system.

France and Greece comment that no legal provision exists for such cases and access would require a judicial appraisal.

However, the Netherlands, Sweden and Italy have made special provision for such cases in their legislation.

There is no provision in Belgium for lawful remote interception of a computer system.

With regard to the question addressed to each national representation regarding the possibility of tapping public or private networks, Germany has quite rightly pointed out that the wording calls for prior definition of the concepts concerned. In fact, distinguishing between networks by economic sector and the nature of the network operators depends to a certain extent on national criteria.

In any case, to attempt to make a clear distinction between the public and the private sector in the corresponding national laws on telecommunications is outside the scope of our objective.

However, the replies given state that there is no legal difference according to the network, except in the case of the Netherlands, Greece and Sweden, which specify public networks as the only area in which interception may take place.

In Finland the law is expected to make an exception for networks for exclusively private use.

Moreover, in the Netherlands the trend towards liberalization of the telecommunications services has consequences for the criminal justice authorities with regard to interception.

B. LEGAL SYSTEM COVERING INTERCEPTION IN THE CONTEXT OF ORDINARY CRIMES

B.1. When the order is given

In most countries, police interception of communications is authorized only if the crime being investigated is on a restricted list of serious criminal offences. At the same time, as a result of the above condition, it is required that the crime being investigated is punishable by penalties greater than 1 year's prison at least, while in Austria an exception is made: telecommunications installations in a multimedia company (press, broadcasting, etc.) may be tapped if a person suspected of a crime punishable by between 5 and 10 or more years' imprisonment uses the installation or tries to establish communication with it.

It should be pointed out that Spanish legislation is drafted more loosely, since neither particular crimes nor the duration of sentences are specified. It is therefore for a judge to decide on the proportionality of an interception measure, which infringes a basic right.

In the case of Norway interception may be requested only for the purpose of investigating national security or drugs trafficking offences.

In most countries, national law grants the power to authorize interception only to a judge. In Austria, Greece and Finland the authorization of a collegial body (a court or council) is also required. In the Netherlands, the public prosecutor may also authorize it. In Germany, Greece, Italy, Norway and Sweden, although the power to order interception generally lies with the judge, in cases of emergency it may be authorized for a limited period of time by the public prosecutor with subsequent judicial ratification being required.

The executive is allowed to order tapping in the United Kingdom (a Secretary of State with the rank of minister) and in Ireland, where only the Minister for Justice can do so.

The legality of prospective, preventive or exploratory tapping, in other words tapping without criminal data or evidence, has been discussed at meetings of the Group. Thus, although it is difficult to establish the stage reached at a given moment in the commission of the crime investigated Belgium, Denmark, the Netherlands, the United Kingdom and Sweden reply that interception may be effected from the preparatory stage, before a police or judicial investigation is opened. We believe that this legal possibility offers great advantages to the police, who can tap people's telephones simply on the grounds of suspicion of criminal activity.

In Belgium neither preventive nor prospective tapping is possible.

In the rest of the countries concerned, an assessment of evidence in order to act is required, in other words, objective data which always give rise to police or judicial enquiries. In this regard Luxembourg lays particular stress on the need for the investigation – which must be under way for interception to be authorized – to be judicial in nature, not merely preliminary. In Austria there has to be some suspicion with evidence of some punishable act. The interception of telecommunications is allowed when it is deemed that this could throw some light on a case. The crime does not have to have been committed. An experimental phase or the commission of a punishable preparatory act is sufficient. A request for telecommunications interception will automatically initiate formal inquiry proceedings ("preliminary proceedings" against known or unknown criminals is not the same as a preliminary inquiry), although the results of the police inquiries are awaited.

There is unanimity regarding the categories of persons to whom the measure may be applied. In general these are the accused, intermediaries or anyone on whom

well-founded suspicions of participating in a crime fall. French law lays down the requirement of informing the Chairman of the Bar Association in cases affecting lawyers. In fact or in law, there is a safeguard which must be taken into account.

With regard to telephones which may be tapped, there is no legal limitation: all those which the competent authority deems appropriate and which are of relevance as regards the person under investigation may be tapped.

B.2. Monitoring during the interception process

With respect to the authorized duration of tapping, Germany, Spain and Ireland all have a maximum time of 3 months, which may be renewed. French law authorizes one month more (i.e., 4) and the law in the United Kingdom and Greece one month less (i.e., only 2) with extensions of one month. Italy is below these figures, with only 15 days, a period which is, of course, renewable.

Denmark, Finland, Norway, Sweden and Luxembourg all have a maximum of one month, renewable for the same period, and in the case of the Netherlands, Portugal and Austria curiously, there is no express legal limit, but the interception order itself must indicate the period of time.

In the Belgian bill of law, the periods proposed are very strict, consisting of two days, renewable for a further two days. The period may be extended to a maximum of eight days by a collegial judicial body. In the case of detection, this period may not exceed two months, unless extended.

Regarding the three questions concerning the recording of the intercepted communications, the persons responsible for checking them and the places where the interceptions are carried out, we have the impression that national laws do not specify these points. These matters are therefore governed by the decisions of the authority (judge, public prosecutor, minister) who orders the interception.

What normally happens is that the aforementioned authority delegates to criminal investigation department or civil service staff the task of recording and transcribing the tapes on their own premises.

In Belgium, the names of the relevant officials or officers of the criminal investigation department must be communicated to the examining magistrate prior to interception and recording.

In the Netherlands and France, public officials not belonging to the police or telecommunications staff may be employed, while in Luxembourg they must be officers from the criminal investigation department.

B.3. "A posteriori" monitoring

A person who is presumed to be guilty is entitled to be informed that a judge has authorized interception of his communications under Article 6.3 of the Convention, in conjunction with Article 8.

Needless to say, such information would jeopardize the result of police investigations, and therefore each country requires a procedural instrument in order to legitimately delay notification of the interested party. Germany, Denmark, Spain, Finland, Luxembourg and the Netherlands (in the future) acknowledge that this obligation legally exists, while at the same time the confidentiality of the investigation must be safeguarded. This obligation is however subject to exceptions in Norway in the case of drugs traffickers.

The Belgian bill of law recognizes the right of the person against whom measures have been taken to be informed of the places and times at which interception occurred, with such notification being given in the preparatory phase or at the conclusion of the criminal investigation proceedings.

The existence of appeal bodies to which the interested party subject to interception

may appeal is a requirement under Article 13 of the Convention.

Admission of the appeals which the suspect subject to interception could bring before the appeal court could have the negative effect for the police investigation of invalidating the proof obtained through the tapping. Sometimes it could even nullify all the other evidence which the prosecution presents, on the basis of the "fruit of the poisonous tree" doctrine. In effect, this means that if evidence is obtained by violation of a fundamental right, not only is this evidence null and void, it also contaminates other evidence from the same source.

Recognition of these appeal bodies is general, except in France, where decisions regarding interception are not judicial.

The juridical role of the legal adviser in Denmark is particularly interesting. Although appointed by the Minister for Justice from among selected, officially appointed lawyers, this person is a private party and defends the interests of the person subjected to the interception measure, by supervising its legality and paying special attention to the grounds on which it is based. If the adviser observes any infringement, he may appeal to a higher court.

However, the most interesting aspect of this legal adviser/lawyer function in Danish legislation is the ban on making contact with the person subject to the tapping. This resolves, in a legally satisfactory way, the problem of maintaining the confidentiality of the police and/or legal investigation whilst ensuring that the interested party's rights are protected.

No special comment need be made about custody of the recordings, except that the Belgian bill states that the clerk of the court is responsible for their custody and their destruction when they are not needed.

C. LEGAL SYSTEM COVERING INTERCEPTIONS IN THE CONTEXT OF ORGANIZED CRIME

It is important to have a special legal system for this type of offence, if only to ensure that the interception order is the responsibility of the administrative authorities, which facilitates the requirements of the police.

Examination of the replies given reveals only one single structured and differentiated legal system. This is the French one, covered by the term "security interceptions".

The power to order the interception lies with the Prime Minister, at the proposal of the Ministers for the Interior, Defence or Customs. The control body is the National Commission, which checks the legality of the tapping at the request of the interested party or on its own initiative.

In Italy there is also a special system for organized crime which includes mafia offences, drug trafficking and terrorism. Although the power to authorize tapping depends on the same authorities – judge and public prosecutor – there are interesting aspects.

These include the fact that under these rules suitable evidence, not necessarily of a serious nature, is all that is needed for interception to be authorized, as in the case of ordinary crimes.

Another feature is the possibility, in cases of emergency, for the public prosecutor himself to agree to interception for a period of 40 days. In these cases interception can be extended directly by the public prosecutor for periods of 20 days.

Finally, perhaps the most interesting feature is that in Italy, under these rules, preventive interception is also allowed; it must always be authorized by a judge, at the request of

the Minister of the Interior, for the purposes of prevention and information, and the results may only be used for the police investigation, not in court.

In Spain the general system provided for in the code of criminal procedure contains one particular feature relating to crimes of terrorism. In such cases the Minister of the Interior, or in his absence the Director of State Security, may take the initiative in agreeing to the interception but the measure may be reviewed, within the following 72 hours, by the competent judge.

In the United Kingdom and Ireland there is only one legal system for any kind of crime and thus, under the heading of "crimes involving State Security", control remains in the hands of the government authorities, the only difference being that the United Kingdom increases the maximum period of tapping to 6 months.

In Norway there exists only one special system for national security and drugs trafficking offences, but by and large this system does not differ from those in respect of ordinary crimes.

The remaining countries do not have a distinct system for organized crime, in the Belgian bill of law typical kinds of crime (drugs and arms trafficking, terrorism, etc.) are included in the general system.

D. LEGAL SYSTEM COVERING NETWORK OPERATORS OR PROVIDERS OF TELECOMMUNICATIONS SERVICES

As regards the existence or otherwise of a legal obligation for operators of networks or services to make interception possible, there are many different replies.

In Germany, Denmark, France, the Netherlands, Italy, Greece, Finland, the United Kingdom, Ireland and Spain this legal provision exists. Specifically, in Germany a decree on the technical implementation of telecommunications surveillance measures regulating the requirements which must be fulfilled by operators and managers of telecommunications installations entered into force as of May 1995. The decree is based on the "international requirements" laid down in ENFOPOL 90 by the Council of the European Union in January 1995, as adjusted to national needs. Future operators and managers of telecommunications installations must fulfil the conditions in order to obtain a licence. Existing telecommunications networks must fulfil the conditions within a certain period. In the Netherlands, providers of telecommunications services have a duty to cooperate if a legal interception order exists; in addition, it is planned to centralize data on subscribers for the benefit of the police authorities so that they can find out quickly whom they have to approach, and a similar system has been discussed for concessionaires and sub-concessionaires of service providers.

In Luxembourg there are no statutory provisions governing such matters.

In Austria, work is currently taking place on a bill (to supplement the Law on Telecommunications) which will be submitted to Parliament this year.

In Belgium, such obligations come under technical assistance.

Both public and private companies are included in this obligation.

The obligation is generally recognized with regard to the data, reports, documentation and questions which complement the interception. In the majority of countries this obligation – which has been established through the telecommunications law or else under the licence to operate granted by the Government to the telecommunications companies – has been especially provided for.

The type of sanction applicable to non-compliance with the aforementioned obligations is not very clear in all cases. In general, penalties of prison and/or a fine are laid down.

As a deterrent, all countries punish with penalties of prison and/or a fine the violation of the confidentiality of communications, in other words, any unauthorized interception whether by a public or private employee. It would therefore seem to be a good idea to have a regulation like the one in France, for monitoring equipment and apparatus technically capable of carrying out interceptions, since it is very important to keep an eye on the means or instruments with which offences can be committed.

The Belgian bill is consistent with this approach and provides for the possibility of regulating by Royal Decree the arrangements for acquiring and trading in technical devices capable of controlling interception, from the manufacturing stage to import or export. There are no provisions for the matter in the other countries.

In Spain a recent amendment to the Penal Code lays down longer sentences and heavier fines for both civil servants and private individuals who violate the confidentiality of communications or carry out unlawful disclosure. A criminal law amendment along these lines is also proposed in Belgium.

With regard to encryption as a special function of telecommunications (question D.7 of the questionnaire should be considered in these terms), once again, two regulatory channels may be opted for. The first involves specific treatment, as is done in France (the law of July 1991 on telephone interception); the second involves establishing either in the Telecommunications Act, as is the case of the United Kingdom (1985 Act), or else in the award of permits in other countries, the obligation to decipher the communication and supply all the relevant data to the authority which requests it.

In general the countries have no specific provisions with regard to encryption.

Finally, the matter of provision for any costs incurred by public or private companies as a result of carrying out interceptions has been thoroughly discussed in Germany. One view is that the total cost should be borne by the operators of the network, while another is that certain costs should be borne by the operators with a part being reimbursed in each case.

Notwithstanding the above, there is provision for reimbursing the network operator for personnel costs and for the use of the transmission channels.

French law does not contain express provision for refunding the expenses incurred but, at the same time, the network operators are obliged to adopt the necessary measures in order to ensure interception.

In the Netherlands a parliamentary decision is expected in the near future. In the other countries it can be deduced that in practice public bodies bear these expenses, provision being made for them in the budgets, but there is no specific legal provision.

Moreover, studies on provision for costs have been carried out recently by the Group

and have made considerable progress since the Bonn meeting (June 1994) with regard to classifying them and charging them to the parties concerned.

CONCLUSIONS

The following conclusions can be drawn from this report:

1. Since there is both protection of the confidentiality of telecommunications and the legal possibility of intercepting them in the course of an investigation, for the purposes of police collaboration attention should be paid to the specific features of each country's legislation.

2. From a legal point of view, and as far as the authorization of interception is concerned, the technical medium used in the telecommunication which is to be tapped is not especially relevant.

   The question of access to computer systems in particular should not be a decisive element in the judicial appraisal. The latter should mainly concentrate on the seriousness of the crime, the need for and proportionality of the measure, what gave rise to it, etc..

3. Generally speaking the nature of the communications network (public or private) does not present any legal obstacles for the purposes of interception.

4. The grounds for interception will be the commission of a serious offence: in general, one punishable with penalties of more than 1 year's imprisonment.

   In Norway such offences must be related exclusively to matters of national security or drugs trafficking.

5. The power to authorize interceptions resides, in continental law, in the hands of the examining magistrate or a court, although this measure may be taken in advance by the public prosecutor in emergencies in some countries.

In English law, this competence for any type of crime (including organized crime) belongs to the highest government authorities (Minister, Secretary of State).

In France, however, these governmental authorities have competence in offences related to national security and organized crime through a differentiated legal system. Some government measures to order interceptions are authorized in Italy in the above cases, and in Spain only in the case of terrorism.

6. The requirements to be fulfilled under the law of each country regarding the stage reached in the commission of the crime being investigated in order for judicial authorization to be granted so that interception may be carried out are of particular interest. In some countries there is considerable flexibility and prospective interception, or interception for information purposes, is allowed, while in others clear and precise evidence, at least, that a crime is being committed is needed.

   Italian law shows a flexible approach: it is stricter regarding the burden of proof with regard to ordinary crimes than with regard to organized crime, which is logical.

7. The maximum authorized duration for tapping fluctuates between 4 months and 15 days, which may be renewed, with the exception of the Netherlands, Portugal and Austria, where the law does not expressly indicate any limit.

   The Belgian bill of law is the most strict in limiting the period to two days, renewable, or to a maximum period of eight days (collegial decision).

8. A successful police operation does not end with the acquisition of an incriminatory recording, but with recognition of this proof as valid before a court. Police action in the phase of obtaining and transcribing the recordings therefore becomes important.

The legal role of the Danish legal adviser may help to reconcile protection of the rights of the person whose communications are intercepted and the success of the police or judicial investigation.

9. Practically all the countries expressly acknowledge in their law the network or service operators' obligation to carry out the necessary operations which make interception possible, and lay down that they must also provide the legally authorized authorities with such additional information as may be required. In other cases this obligation is specified when the operating licence is granted.

10. Although all the countries questioned replied that they have provided for legal sanctions for violation of the confidentiality of telecommunications, they acknowledge, however, that the State does not have control over equipment and apparatus capable of intercepting them (with the exception of France and Belgium (legal provision not implemented)).

11. To date there has been very little development in rules governing encryption as a special function of telecommunications.

12. Generally speaking, there are no rules laid down with regard to costs arising from interception or the classification and charging of such costs to the parties concerned.

RECOMMENDATIONS OR DRAFT DECISIONS

There is much to be learnt from studying the comparative law applicable to the subject under study in respect of legal principles, rules or techniques successfully adopted for the solving of common problems. We therefore consider it desirable to recommend the following:

1. As regards the legal system:

The legal provision under national law of a legal system which, without diminishing judicial control, grants the maximum initiative to government authorities during the different phases of telecommunications interceptions as an extremely valuable way of gathering evidence in the fight against organized crime.

In some countries, extraordinary powers have been conferred on the public prosecutor for the specific purpose of combating this type of crime, and in other cases for reasons of urgency.

2. In the criminal proceedings area:

   - Study of the introduction of telecommunications interception from the preparatory phase to commission of the crime (preventive or prospective tapping).

   - Examination of the interesting role fulfilled by the Danish legal adviser, inasmuch as he guarantees the rights of the person subjected to interception, without reducing its effectiveness from a police point of view.

3. In the administrative area:

   - Include in telecommunications legislation, regulations and licensing conditions the obligation for network operators and service providers to carry out complementary operations to facilitate interception and help provide any relevant data requested.

   - Organize State control of apparatus and equipment capable of intercepting telecommunications.

4. In general:

- It is desirable that a determined legislative effort be made, which will have to be harmonized in order to keep police collaboration active and fruitful in the area of telecommunications interception, where technical developments are determining priorities in certain countries.

  The operational requirements laid down by the authorities and police officers to tackle ordinary crime, as well as organized crime, need to have a harmonized legal framework in order for international police cooperation to be effective.