2000

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

PC-S-CO (2000) 3

Report on Interception of Communication and Intrusive Surveillance[1]

(Best Practice Survey No. 3)

[1] Adopted by Committee PC-CO at its 4th meeting (1-3 December 1999).

Strasbourg, 15 March 2000 PC-S-CO (2000) 3

EUROPEAN COMMITTEE OF CRIME PROBLEMS
(CDPC)

Group of Specialists on Criminal Law and
Criminological Aspects of Organised crime
(PC-S-CO)

Report on Interception of Communication and Intrusive Surveillance

(Best Practice Survey No. 3)

Contents

1. Introduction

1.1 Background of the project

The Committee of Experts on Criminal Law and Criminological Aspects of Organised Crime was established in 1997. Its terms of reference, adopted by the Committee of Ministers at their 587th. meeting on 1 April 1997, state that the Committee should - *inter alia* - study existing solutions to combat organised crime in Member States, that could serve as examples for other Member States. In order to fulfil this assignment the Committee decided to carry out a series of best practice studies. One of these concerns a survey on interception of communications, intrusive surveillance and some other, more or less similar, investigative methods. This topic was chosen because:

- due to the very nature of the organised crime, i.e. the fact that criminal activities are planned and conducted within the closed group of actors taking often various special precautions against detection of such activities, traditional means of collecting evidence used in cases of other criminal offences, such as witnesses and experts testimonies or material evidence, are very often of less or even no value;

- because of this it is essential to the police's and other law enforcement agencies' activities aimed at disturbing activities of criminal groups and collecting evidence that could lead to convictions in courts, to obtain "insider knowledge" about activities of such groups. However, this is often a very difficult task, which may be realised only using special investigative techniques and special investigative equipment, making possible either interception of telephone, fax or Internet communications (interception of communications), or making audio or video recordings of conversations or events taking place in particular places or rooms, tracing movements of persons, cars etc. (intrusive surveillance).

- modern technology seems to offer nowadays almost unlimited possibilities. However, it is not primarily the technological, but foremost the ethical and legal, including constitutional, barriers to such activities which are subject to a very intensive discussion, controversy, and sometimes strong objections, in many contemporary democratic societies. Although it would be by any means an overstatement to claim that some sort of "1984 syndrome" endangers the rule of law in modern democracies, there is no doubt that the aims of protecting privacy of citizens and combating effectively certain forms of criminal activities may result in many tensions and conflicts.

1.2 Purpose of the study

One of the major functions of the system of criminal procedure in a democratic system adhering to the principle of the rule of law, is to protect not only persons suspected or accused of committing offences, but also innocent citizens, against governments' arbitrary actions constituting infringements of basic human rights, against undue intrusion in their private lives, and against other

forms of abuse of power by the State. As a matter of fact, the evolution of the modern systems of criminal procedure since the beginning of the twentieth century constituted a process of constant strengthening of various legislative guarantees against such abuses. Such guarantees most often acquired a constitutional character, or became even norms of an international character. The European Convention on Human Rights and its system of enforcement constitutes the best example of this.

Although tensions between the need to protect legitimate rights and liberties of the accused and citizens and the need to make the fight against crime effective have always existed, growing problems with organised criminality, which may be observed all over the world for some twenty years, seem to increase these tensions. As mentioned above, because of the very nature of the organised crime, as a group activity taking place within the special milieu which considers secrecy and clandestine activities as one of the most important precautions, investigating offences committed by such groups and securing evidence for trial, constitutes a major challenge for law enforcement agencies. It means that to be effective in this field, law enforcement agencies cannot rely any more exclusively on traditional, reactive methods of policing and investigating, which were relatively effective to combat street crime. They have to use to a much greater extent a variety of more pro-active and intrusive methods, which may penetrate very deeply into the sphere of privacy, not only of suspects, but also of members of their families and acquaintances, and individuals having no relation whatsoever to the target persons or to any criminal activity perpetrated by these suspects.

However, growing pressure to introduce such methods or to "liberalise" rules of their admissibility, meets sometimes with strong objections on the side of civil libertarians. This may be especially strong a case in the countries of Central and Eastern Europe which remained for many years under the totalitarian rule. The problem is that under totalitarian regimes, such methods are usually used or abused widely for political purposes, to control and persecute political opponents, real or imagined ones. For many people in these countries, but not only there, the interception of private communications by the police or the bugging of apartments or hotels are synonyms to the methods adopted by totalitarian police states and not by democratic societies governed by the rule of law. Many people in these countries were fighting very long to make such abuses of State power impossible. Re-introducing them now, even accompanied by a variety of safeguards and restrictions, is perceived sometimes with great suspicion. Although nowadays there is no question that the use of intrusive policing methods is indispensable to fight the menace of organised crime effectively, one should not forget the possible negative side effects arising from their application.

Of course, it is obvious that there is a basic difference between using such methods by unaccountable regimes and applying them in a democratic society which has a variety of safeguards against the abuse of State powers. However, using intrusive policing methods poses always special problems, even in most open and democratic societies, as such methods are always prone to abuse. The basic problem is that in order for such methods to be effective, they have to be applied during the investigation in secret. Only in such circumstances will they be effective and bring the results sought. This means however, that procedures adopted to apply special investigative methods are of a very low visibility. To be effective in this area, the police have to be as secret as possible, which makes advance accountability and public control very difficult or sometimes even impossible. Such a situation on the one hand is prone to various abuses, while, on

the other hand, it may result in public fears of the police being too intrusive and out of effective control. Under such circumstances, it is very important to strike a proper balance, both in legislation and in practice, between the various conflicting needs and values in question. The main purpose of this study is to provide information on how the three chosen Member States of the Council of Europe deal in their legislation and practice with finding this balance. The level of aspiration does not go beyond an attempt to provide both these and other Member States of the Council of Europe a number of suggestions and guidelines on how to fight organised crime more effectively by using covert police methods, while at the same time basic human rights are respected and protected as much and as far as possible.

1.3 Definitions

For the purpose of this best practice study, the following definitions are used.

- Organised crime means[2]: *the illegal activities carried out by structured groups of three or more persons existing for a prolonged period of time and having the aim of committing serious crimes through concerted action by using intimidation, violence, corruption or other means in order to obtain, directly or indirectly, a financial or other material benefit.*

- Law enforcement officials means: *all officers of the law, whether appointed or elected, who exercise police powers, especially the powers of using investigative methods.*

- A special investigative method is: *a way of gathering information systematically in such a way as not to alert the target person(s), applied by law enforcement officials for the purpose of detecting and investigating crimes and suspects.*

- Interception of communication is: *the covert monitoring of direct communication or telecommunication in which one or more suspects are taking part, in order to provide evidence or intelligence on their participation in crime.*

- Intrusive surveillance is: *the covert monitoring of the movements of suspects by watching or listening in person and electronically in private places, in order to provide evidence or intelligence on their participation in crime.*

1.4 Fieldwork

The situation regarding interception of communications, intrusive surveillance and other similar special investigative methods was studied in three countries: Hungary, Turkey and the United Kingdom[3]. These Member States were selected on the basis of the following considerations:

---

[2] See the (draft) Recommendation No. R (2000) ... of the Committee of Ministers to Member States concerning guiding principles on the fight against organised crime.

[3] The authorities which have been met have kindly accepted that the names of the countries be mentioned in the introduction of the report, on the basis of reciprocity

- they all experience problems because of the illegal activities of organised criminal groups;
- they have different legal systems;
- there differ significantly in aspects like geography, history and culture;
- it was expected that, mainly due to the differences mentioned above, they varied in both legislation and practice concerning the use of special investigative methods.

The three member States selected for this best practice survey were visited in October 1999 by a small delegation of the Committee. The delegation was composed of Mr. Christophe Speckbacher, Division of Crime Problems, Adviser to the Program Octopus II, Mr. Toon van der Heijden, scientific expert of the Committee PC-CO and Mr. Krzysztof Krajewski, member of the Committee PC-CO. In every country the delegation visited law enforcement agencies (police units and competent agencies within the respective ministries of interior). In two of them interviews were conducted also with prosecutorial and judicial authorities.[4] The main purpose of the interviews was always to obtain first of all information about the legal framework of the activities constituting the subject matter of the survey and than to gain some insights into the problems connected with practical application of these laws and practical aspects of the law enforcement agencies' activities in this field.

In addition to the interviews, relevant documents, mainly provided for by respondents and for the rest resulting from a limited search in literature, were studied. On the basis of this material, this report was written. The responsibility for the contents of the report lies with Toon van der Heijden and Krzysztof Krajewski. The views expressed do not necessarily represent the official views of the Council of Europe.

The authors would like to emphasise that this survey is not meant to be a comprehensive study on special investigative methods. We hope the results nevertheless provide arguments for the introduction of changes which will result in a more harmonised legal practice regarding the use of covert investigative methods in member States of the Council of Europe.

1.5 Characteristics of the legal systems of the Member States surveyed

The legal systems of the three Member States under survey belong to different legal traditions. Two of them belong to the continental tradition, what means that their systems of criminal procedure may be described as moderately inquisitorial or mixed ones. The legal system of the third country belongs to the common-law tradition, i.e. its criminal process may be described as adversarial one. It means first of all that there are sometimes important differences between two first and third country with respect to the role played by the investigation and the role played by the trial phase of the criminal process.

In all three countries, investigation constitutes a phase devoted to revealing offences, detecting their perpetrators and discovering and preserving evidence for the future use by a criminal court during trial. There are however major differences in how this task is realised. Under the inquisitorial system, one of the major problems is the relationship between the police and the public prosecutor. Although investigative activities are conducted in principle, also because of

[4] The Committee PC-CO would like to thank all the people who were interviewed for this best practice survey.

purely “technical” reasons, first of all by the police, an important role is played by the public prosecutor, who has the general right to oversee the entire pre-trial proceedings. It means that the police have at least the duty to inform the public prosecutor about every new case they investigate and to provide her/him with all relevant information about their activities. The public prosecutor usually has the right to interfere at any time with the activities of the police. He or she can conduct major or all of the investigative activities her/himself and makes major decisions during the proceedings. In one of the countries under survey, a major reform of the criminal procedure is underway, which includes among others strengthening of the powers of the public prosecutor during the investigation. It is also the public prosecutor, and not the police, who, after evaluating the results of the investigation, makes a decision about bringing an indictment to the court, discontinuing the proceedings or terminating it in any other way specified by the law. Despite the fact that the public prosecutor later, during the trial, constitutes a party supporting the indictment, during the investigation he/she plays by no means an exclusively partisan role. It means that the main task of the police and prosecutorial during the investigation under inquisitorial system is not to collect evidence against the suspect but rather to investigate the case fully and objectively, to collect and preserve any piece of evidence which makes it possible to establish the material truth about it. In that capacity, the prosecutor plays also the role of the guardian of the rule of law. Although in neither of the two countries is the institution of the investigating judge (magistrate) known, some major, most intrusive decisions (e.g. preliminary detention of the suspect), are taken during the investigation by the court (judge) and not by the public prosecutor.

The trial phase in the systems of the two countries under survey is dominated by the presiding judge. It is s/he who examines witnesses and experts, and takes other evidence. He/she has the duty to guarantee that all aspects of the case are considered, all available and necessary evidentiary possibilities used and objective truth is revealed during the trial. Although the judge has in such a system the possibility to introduce any piece of evidence he/she considers fit, he/she usually relies heavily on the dossier of the case, which was composed during the investigation by the police and prosecutor. The trial parties, i.e. the prosecution and the defence, although they have broad possibilities to act, remain under such system relatively passive and play only a secondary role. There is also no participation of a jury in either of the two countries.

Counter to that, in the country using an adversarial system of criminal procedure, the investigation is in practice a sole responsibility of the police. Although police have the duty to disclose any piece of evidence collected during the investigation to the accused and his/her defence, it is rather the defence’s role to collect evidence exculpating the accused or mitigating his/her responsibility. The adversarial character of the proceedings also means that there are some problems with any possible judicial intervention in that phase of the proceedings. Despite the fact, that both inquisitorial and adversarial system adhere to the principle of immediacy, this principle in general is of greater importance under the adversarial system. It means also that during the trial phase it is parties who introduce and present evidence, examine and cross-examine witnesses etc. The presiding judge is playing a more passive role. Although he may ask any questions and may initiate the introduction of new evidence, this is left rather to the large extent to the parties. It is important also that, at least some cases under the adversarial system are tried with the participation of a jury.

1.6 Interception of communications and other intrusive methods from the point of view of the European Convention and Court of Human Rights

The relevant case law, mainly based on Articles 8 and 13 of the European Convention on Human Rights, has highlighted several principles in favour of the state authority, according to article 8 paragraph 2. It has also clarified limits in favour of individuals subject to electronic surveillance in the broad sense. The main cases relating to interception of communications (other than mail) and secret surveillance are Klass (1978), Malone (1984), Leander (1987), Huvig and Kruslin (1990), Lüdi (1992), A. against France (1993), Halford (1997), Kopp (1998). They refer to the necessity of a legal framework and to its content, adequacy and proportionality of the measures, modalities of interception and surveillance, authorisation procedure, existence of effective remedies, the question of information storage among others. But other rights (freedom of expression or association) also set limits with regard to the fight against organised crime. In determining exactly the degree of acceptability of surveillance measures by the European Court, one should therefore take account of the evolution of the case-law.

It seems useful to quote the text of the relevant provisions in the Convention:

"Article 8 – Right to respect for private and family life

1 Everyone has the right to respect for his private and family life, his home and his correspondence.

2 There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

"Article 13 – Right to an effective remedy

Everyone whose rights and freedoms as set forth in this Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity."

2. Findings

2.1 Scope of application

In the three countries that were subject to this best practice survey, interception of communications, intrusive surveillance and other similar investigative methods may be used only to investigate certain serious offences, what means that the legislator in these countries tries to held some balance or proportionality between the use of intrusive methods and the gravity of the offence under investigation. In other words it doesn't seem to be appropriate in any of the three States to apply such drastic methods to investigate petty offences.

In the first of the countries under survey, both interception of communications and intrusive surveillance are permissible only in two areas regulated in two special, separate pieces of legislation. The first one, which is in force for about twenty years, refers to acts of terrorism, and the second one to what is called profit-oriented criminal organisations. This last act is quite new, as it is in force since July 1999 only, what means also that there are relatively few practical experiences with its application. All that means that before the law on the profit-oriented criminal organisations entered into force, there were no formal possibilities of intercepting communications in that country, except in terrorism cases. This resulted in legal and practical problems and discussions about the applicability of such measures because of the constitutional provisions which guarantee secrecy of the telecommunications with exception for the purposes of the law enforcement. There are strong indications that covert police methods were used in this country in cases of profit-oriented crime, like drugs trafficking, for many years before the new law came into force. It was argued that in these cases the proceeds of crime were meant for the financing of terrorist activities. The highest judicial authorities tolerated the investigative methods as long as there was no provocation to commit a crime.

For the purposes of this study only the legal basis for the use of covert methods against profit-oriented criminal organisations is of relevance. The new legislation applies to any person who establishes, directs, or acts on behalf of a criminal organisation which has certain specific tasks or purposes (e.g. controlling or influencing institutions, enterprises, public administration or services, media, obtaining illegitimate profits, etc.), or applies certain special methods (e.g. uses violence or threatens to use violence etc.). The law provides not only criminal punishment for such activities but also various procedural measures to investigate them. It means that in this country interception of communications and intrusive surveillance as investigative measures are connected directly to serious and organised crime (and terrorism) problems. It seems that in cases of 'ordinary' offences, interception of communications and intrusive surveillance are not possible under the law. However, organised crime is defined rather broadly. The law on profit oriented criminal organisations not only refers to traffic of narcotics drugs; there is extension of wiretapping powers to cases trading with arms and art objects, cultural inheritance or environmental protection if committed in an organised manner.

The second of the three member States surveyed belongs to the group of the former communist countries, what means that the legal profession and public in general are very sensitive about adoption of such measures as interception of communications or intrusive surveillance which were widely abused earlier for political purposes. Because of this, special investigative techniques are dealt with in a comprehensive manner in the special law which regulates operations of the police. This law contains a special chapter dealing with various methods of secret data collection, which is of a quite detailed character and lists and regulates various police techniques permissible under it. Such techniques may be used to prevent or detect criminal offences, to interrupt their commission, to determine the identity of criminals, apprehend them, etc. Although many of them are permissible in investigating any offence, intercepting and recording of the contents of telephone conversations or fax or Internet transmissions, and audio or video recording of events taking place on private premises is permissible only in cases of grave criminal offences (this does not include matters of national security, which are dealt with separately in the same law). Although the law under discussion does not define explicitly what constitutes a grave offence, it is understood that

such character is attributed to offences threatened with the maximum penalty of no less than 5 years of imprisonment. Additionally the same law contains a provision which permits adoption of the methods mentioned above in cases of other offences, i.e. even if they are threatened with a lower minimum statutory punishment. The law contains a detailed list of such offences, which includes also offences of an organised character, such as drugs trafficking and counterfeiting money. Furthermore, the list refers to any criminal offence that is directed toward a child, perpetrated armed or connected to international crime. A special provision relates to cases in which a user of a telephone is seriously threatened or instigated to crime and s/he requests help. In such a case the police may have access to the contents of the communication relayed by the apparatus and may record it without judicial permission.

Finally in the third country interception of communications and intrusive surveillance are dealt with in two separate pieces of legislation. Interception of communications transmitted by means of public telecommunications systems is regulated in special piece of legislation dealing exclusively with this method. Apart from the cases of national security, and such involving the economic well-being of the country, it is permissible to apply such measures also for the purposes of preventing or detecting serious crime. Although the law does not define clearly this term, it seems that practical standards are rather high and provisions are applied primarily in serious organised offences, first of all drug cases. On the other hand regulations on intrusive surveillance are dealt with in the law regulating police's activities and refer also to the concept of serious crime. It is important here, however, that in that piece of legislation this term is defined in a more precise way by the reference to such elements as use of violence, substantial financial gain or group character of an offence under investigation, and the minimum sentence expected for such an offence when brought to court.

The main forces behind the developments in that country seem to be the privatisation of telecommunications companies and technological developments like the expansion of the Internet. A second development is the changing practice of criminal investigation: from reactive to pro-active, also called "intelligence driven", which stimulates the use of sophisticated covert techniques. Another relevant development was a series of judicial decisions, especially by the European Court of Human Rights, which made clear that the present statutory law does not provide an adequate legal framework for the interception of non-public telecommunications networks. Domestic and European court decisions in the recent past have led to a small amount of legislation of an *ad hoc* character. The distinction between public and private networks also causes an inconsistent regime for the interception of electronic mail. Furthermore, the present legislation knows different regimes for the interception of (public) telephone communications and wireless telegraphy. Because of all this the government of that country recently has expressed the will to come to a single legal framework which deals with all interception of communications, regardless of the means of communication, method of licensing and the way the communication is being intercepted.

2.2 Additional requirements

In two of the surveyed countries there are certain additional safeguards and requirements attached to the provisions on admissibility of intercepting communications or using intrusive surveillance, which can be called the principle of subsidiarity. It means that such measures can be

applied only if it would be impossible to achieve tasks of the investigation by other means. In one of those two countries, there is even further stipulation placing additional limits, namely requirement that the results of such action are likely to be of substantial value to achieve the goals of the ongoing investigation. In other words, interception of communications and intrusive surveillance methods cannot be applied to realise tasks of minor importance from the point of view of the primary goals of the investigation.

It is interesting that only in one of the countries in the survey there is clear cut provision that application of interception and tapping of communications requires prior strong indications that an offence has been or could be committed. There are no similar provisions in two other countries. It is obvious, however, that general principles of criminal procedure apply here and it is impossible to use such measures without any ground or only because of rumours, hearsay, general suspicions (based for example on previous convictions only) etc. This is due to the fact that in those countries it is not the police itself who decides whether to use or not such measures. Police have usually to apply in such cases to some other authority and because of this have to substantiate their application also in terms of the evidentiary grounds for such application.

2.3 Agencies deciding on application

As mentioned above, in all three countries under survey it is not the police who decides on the application of such measures. With some exceptions, for cases of emergency, in all three of them it is a judicial authority or some high ranking official in the ministry of interior. Especially the involvement of the judiciary constitutes here very important element constituting a basic safeguard against eventual abuse and infringement on civil rights.

In the first of the surveyed countries, decisions on the application of the interception of telecommunications and tapping of them constitute the exclusive competence of the judge. This also applies to other methods of intrusive surveillance, such as static or dynamic surveillance and making video or audio recordings of the activities of a suspected person. Such methods are permissible, both on public and private premises, and may be applied in case there are strong indications that the target person is involved in organised crime.

A more or less similar situation exists in the second country. Interception of communications transmitted via telephone, fax or the Internet always requires judicial approval, with the exception of matters of national security, which are beyond the scope of this study. On the other hand, the situation with respect to intrusive surveillance differs, depending on whether actions should take place on private or public premises. Surveillance does not require judicial approval if conducted on public premises. Observation and recording (audio or video) of events taking place on private premises (static surveillance) is permissible, but has also to be accepted by the judge. It is necessary to underline that the discussed law in this country contains a legal definition of private premises. There is also an exception to the rule that application of such measures requires judicial approval. Namely, in cases of certain offences, like for example extortion or blackmail, if the person threatened by such offences requests in written that the police intercept and tap his/her telephone, judicial approval of such measures is not necessary.

In the third of the surveyed countries, there is also a difference with respect to approvals of intercepting communications and of intrusive surveillance. Namely, intercepting communications transmitted on public telecommunications systems does not require judicial approval, but a warrant which is issued personally by the minister of interior. On the other hand, any method of intrusive surveillance which requires interference with property or wireless telegraphy requires proper authorisation in writing. Such authorisation may be given only by certain high ranking police officers listed in the law. In specific cases of intrusive surveillance there are further important requirements. In case a given action is to take place on certain types of private premises specified in the law (like dwelling houses or hotel bedrooms), or it is likely that this action will result in obtaining access to certain types of information (protected by special privileges), the authorisation issued by the police has to be approved by a special officer of judicial qualifications (from the special panel of such officers nominated according to special procedure). In this country there is also an independent board, comprised of officers of similar high status, which handles complaints of individuals regarding the use of covert investigative methods.

2.4 Procedure in cases of emergency

The legal system of all three countries provides for special procedures in using interception of communications or other methods of intrusive surveillance in cases of emergency, i.e. in such cases when delay in their application resulting from adherence to standard procedures of authorisation and approval (which take always some time) may result in the evidence being lost, distorted or useless. Such procedures for cases of emergency are usually substantially simplified, what means that it is possible to take appropriate action without authorisation necessary on regular basis. Interception of communications or intrusive surveillance ordered in such extraordinary way may be conducted however only for certain, usually rather short, period of time. Within this period it is also necessary to obtain authorisation or approval according to regular procedure and action may be continued beyond this emergency period specified by the law only with such regular approval or permission. If such approval or permission is refused action has to be discontinued immediately and all materials obtained have to be destroyed within the period specified under every legal system.

For example, in the first country emergency application for the interception of communications may be ordered by the public prosecutor, not by the police. Such emergency application is permissible for 24 hours only. If judicial approval is refused all data have to be destroyed within 10 days. In the second country intercepting of communications or intrusive surveillance which require judicial acceptance are possible in emergency situations without such acceptance for the period of 72 hours. The decision may be taken by the head of the police unit competent for the given investigation. Finally, in the third country intercepting communications transmitted on public telecommunications systems in emergency cases requires also a warrant which may be issued, however, by an official of the lower rank than the minister of interior, but not below a certain rank within this ministry. Such a warrant is valid for two working days only and continuation of interception beyond this time period requires a new warrant, issued according to the regular procedures. With respect to other measures of intrusive surveillance, the legal system of the third country provides that in emergency cases oral authorisation by the mentioned above high ranking police officer may suffice. Again, intrusive surveillance measures may be applied on the base of such authorisation for 72 hours only. Their continuation requires the normal approval

procedure.

2.5 Duration of the application of special measures

In all three countries under survey law provides certain time limitations on the application of either interception of communications or intrusive surveillance. In the first country judge while authorising the use of such measures may originally permit interception of communications for three months. This time period may be extended, but only twice, each time for additional three months. Extension of the application of such measures requires always judicial decision. It means that interception of communications (against the same person) may be applied for a maximum period of nine months which cannot be extended any more. On the other hand other methods of intrusive surveillance may be under the legal system of that country applied indefinitely.

It is also in the second country where original authorisation for interception of communications may be issued by the judge for 90 days. This applies however also to intrusive surveillance on private premises, as such measures require in that country also judicial approval. This time period may be extended for another 90 days (also by judicial decision). It is important that, due to the unclear formulation in the text of the law, there seems to be certain dispute about provisions applying to this extension. On its face it seems that such extensions may be granted every 90 days indefinitely, i.e. there is no maximum time limit for applying intrusive measures. Some support however the opinion that such extension may be granted only once, what would mean that interception of communications and other measures of intrusive surveillance requiring judicial approval may be applied for a maximum period of 180 days.

Finally in the third country different limitations apply to the interception of communications transmitted on public telecommunications systems and to the intrusive surveillance. In the first case original warrant may be issued by the minister of interior for the period of two months. This may be prolonged depending on the grounds justifying its application. In cases of serious offences (which include offences of organised crime) extension may be granted for one additional month only. In cases pertaining to national security matters and economic well-being of the country it may be six months. On the other hand authorisation to apply other measures of intrusive surveillance may be granted for the original period of three months. This period may be extended by another three months. It is important to note that in such cases renewal may be granted unlimited number of times. It means that as opposed to interception of communications transmitted on public telecommunications systems, which in cases of serious offences cannot extend three months, other intrusive measures may be applied (at least theoretically) indefinitely.

It must be also stressed that in all three countries there are provisions which require interception of communications or intrusive surveillance measures to cease to be applied immediately if the goals for which they were applied were achieved (e.g. necessary evidence was obtained). This shall prohibit unnecessary continuation of such measures beyond the needs of criminal investigation.

2.6 Scope of targeting

One of the most important problems, both legal and practical, relating to the application of

the interception of communications and intrusive surveillance measures is the fact that it is not only suspected criminals who may be subjected to such measures. Their application means that investigating officials may also obtain information and material relating not only to family members and acquaintances of the target persons, but often to persons having no relation whatsoever to such persons, whose connection with them or with the case may be absolutely accidental. This may not only rise serious concerns from the point of view of protecting the right to privacy, but also cause various problems, namely how such additional information has to be handled and how it may be used.

Because of the mentioned above problems legal systems of the three countries under the survey require usually that authorisations or warrants permitting application of the special investigative methods have to specify target(s) of such measures. In the first country the law provides that warrant shall always specify the name of the target person and the location of the application of special measures (what in practice means either telephone or fax number, or e-mail address in cases of intercepting communications, or rooms, premises etc. to which intrusive surveillance measures shall be applied). In practice in the area of intercepting communications judicial approvals are issued usually for concrete telephone numbers of concrete persons and communication incoming to or outgoing from the target person. However, recently judges seem to interpret these provisions in a less restrictive way and issue approvals for all conversations incoming to or outgoing from the specified telephone number. In such case all information irrelevant for the case under investigation and data on persons not involved in it have to be deleted within 8 days (what is regulated explicitly in the law of that country).

In the second country, judicial decisions on applying interception of communications are issued usually with respect to a concrete person, what means that all telephone conversations of such person from all telephone numbers used by him/her may be tapped. However, authorisation may apply also to a concrete telephone number. There are no clear cut provisions on how to handle other materials gathered or recorded while intercepting communications of the target person (i.e. regarding other, uninvolved persons). The law regulates only such situation in which intercepting communications did not confirm initial suspicion. In such situation interception shall be stopped and all materials deleted within 10 days. It seems that this provision may be applied *per analogiam* to the situation discussed above. In practice, when the police is investigating organised crime, the application for the interception of communication is prepared according to the schedule and planning of the investigation and mentions the core members (or even all members) of the criminal group targeted.

The most complicated situation exists currently in the third country, as warrants to intercept communications transmitted on public telephone systems are issued here not always for persons (although the individual has to be identified in such a warrant) but for telephone numbers. However, law enforcement officers who are listening to the conversation are obliged to switch off the line and the recorder immediately when they notice that an individual who is not the target is using the telephone. Due to the developments on the telecommunications market (technological progress and privatisation), which has resulted in a situation in which one person may use many telephone numbers and/or switch quickly to other operators, the present regulations lead to serious practical problems for law enforcement. Because of this, the government has proposed changes, so that in the future warrants specify the target person, and include a schedule listing of all telephone

numbers which can be intercepted in relation to that person.

2.7 Spatial application

A crucial element in respect to spatial requirements is the differentiation between public and private premises. For example, in all three countries under survey it is in principle possible to use intrusive measures on public premises. It may include also intercepting telephone conversations from public telephone if there are grounds to assume that this telephone is used for criminal purposes (such situation exists in one of the countries). It means, that restrictions apply normally to such interceptions of communications and first of all intrusive surveillance measures which take place on private premises (at least this differentiation is clearly specified in the legal systems of the other two countries). Of course of crucial importance for this differentiation is to have clear a definition of what may constitute private premises. For example the definition mentioned earlier contained in the legal system of the second country is limited to a private residence, what *a contrario* means a rather broad understanding of the term public premises. Also the legal system of the third country contains a rather detailed definition of what has to be treated as places or premises subject to special protection.

Regarding the interception of mobile telephones, there are no major legal obstacles. In only one country it was noted that legal problems hindered the tapping of a specific type of phones. However, in practice there are technical problems with the interception of mobile telephones in all three countries in the survey. Furthermore, financial obstacles were observed in two of the three member States. Both types of problems were aggravated as a result of the increasing number of private telecommunication (including Internet-) providers, since interception facilities were considered necessary for each provider individually. In one country there was an ongoing discussion on how far the legal obligation of a private telecom provider should go in establishing such facilities. In the other two member States there already is a formal obligation for telephone companies and other telecom providers to co-operate with law enforcement. However, in one of these two, an obstacle is encountered if the provider involved does not have a seat in the country, since such a provider can not be forced to co-operate. It is not clear whether or not these providers refuse to co-operate with the law enforcement authorities in this country. In practice it does not seem to be a big problem, presumably because these foreign providers do not have a large share of the market. However, since the telecom market is very dynamic, this situation might change in the near future.

Another problem concerns encryption of telecommunication. The deployment of encryption makes it difficult, if not impossible, to make use of intercepted material. Although at the moment it does not seem to be a big problem in the three member States in the survey, it was generally expected to become a major obstacle for law enforcement in the near future. There are indications that some Internet Service Providers will make encryption tools more easily available. Also the use of encrypted mobile phones potentially reduces the information that can be derived from lawfully intercepted communication. One can expect that especially highly sophisticated criminal organisations will try and make use of this opportunity. Although encryption is a world-wide development, only in one of the three member States the government has acknowledged its seriousness and is actively involved in a discussion with relevant domestic partners from the business world and law enforcement. So far, this has led to a discarding of the introduction of a

legal obligation for providers to deposit data encryption keys. Instead, the solution is sought in placing the onus on the recipient of a disclosure notice to prove to the authorities that the requested keys are not in his possession, and to state to the best of his knowledge where they are.

2.8 Frequency and duration in practice

In all three member States in the survey, there were only some statistics available on the actual number of applications and the average duration of interception of communications.

In one of the countries, there were approximately 34 warrants per million inhabitants for the interception of communication in 1998. It was estimated that in 1999, the number would increase about 25%. Covert investigative methods are used especially for combating serious and organised crime. In an unknown number of cases, a warrant refers to intercepting the communication of more than one individual.

In another country, there were about 4 authorisations for telephone tapping per million inhabitants in 1997. In the capital of this country, at least five major organised crime groups recently were dissolved with the help of the interception of communications. The average period of wiretapping currently lies between 1.5 and 2 months.

In the third member State, statistical data was available only on the number of requests at one court in the capital. This court got two to three requests for wiretapping a week. The majority of cases refer to organise crime cases, which involves an estimated average of 10 suspects and 20 offences. Usually the duration is between two and three months. For the whole country it was estimated that special investigative methods are used in approximately one of every 600 investigations. This means that annually about 100 warrants per million inhabitants are issued.

2.9 Disclosure and redress

Disclosure issues may raise very important questions, as information on the application of such measures constitutes for a target person a necessary precondition for the eventual use of recourse, appeal etc. It is obvious, that before and during the application of such measures, the target person shall not be informed about their application, as it would be against the very purpose of these measures. It may be also, that the target person learns about him/her having been or still being subject to such measures later, namely after the investigation has been completed, when he/she has normally the right to acquaint him/herself with the content of the dossier. However, the last situation will occur only, if materials gathered with the help of special measures are included in the dossier as evidence. This means, that there may be a problem, whether authorities have the duty to inform target person that he/she was subject to such measures independently of the fact how materials gathered were used and whether or not an indictment was prepared.

In the first country under survey, there is no disclosure duty under the law, what implicates that the target person may never learn about him/her being subject to the interception of communications or similar measures. There are no provisions for compensation to an individual whose telephone was tapped unjustified. If evidence is derived from the tap, this will be in the file

that is open to the defence.

In the second country, if criminal proceedings have not been instituted, the target person has to be informed about the use of covert methods. However, there is no possibility to appeal to the judicial decision on the application of such measures, even *ex post*. There is only the possibility of a compensation to the target person. If a trial is initiated, the existence of undercover operations and methods should remain secret unless the results are officially introduced as evidence.

In the third country, the situation differs again depending on whether we have to do with the interception of communications transmitted on public telecommunications systems or with intrusive surveillance measures. In the first case, there is a special tribunal established under the law and any person who believes being subject to interception of communications may apply to the tribunal to investigate his/her case. However, there is no duty to inform target persons about the application of such measures. On the contrary, there is even a provision in the law that prohibits the disclosure in court of the application of the tapping of a public telephone system. In practice this makes it difficult, if not impossible, for a defendant as well as for an ordinary member of the public who suspects his or her telephone communication is unjustifiably being intercepted to successfully complain about police conduct in this context. It also leads to the exclusion of evidence which could be vital for the outcome of the criminal trial. Sometimes even strong cases against major criminals have to be dropped in order to prevent the defence discovering the use of telephone tapping by the police. In the second case (i.e. intrusive surveillance) there is no such duty either. Again, there is, a special procedure for complaints by persons who believe to be, or having been, subject to such measures. Additionally, police officers who authorise intrusive surveillance measures may appeal to judicial decisions which refuse to approve them.

One way of monitoring the use of secret investigative methods is the publication of national reports on an annual basis. In only one of the three member States this is common practice. Such reports may help to keep the confidence of the general public in the way law enforcement operates with regard to these methods.

2.10 Use of intercepted material

One of the crucial legal issues with respect to interception of communications and intrusive surveillance constitute the evidentiary value of the materials gathered with such methods, i.e. the question whether they may be treated as intelligence only or may be used as evidence in court as well.

In two of the three countries surveyed such materials may be always used as evidence in court. In one of these, only since about one year information collected by covert investigative methods is presented as evidence during the trial. This policy change resulted in a shock among organised criminals, but is generally considered to lead to more convictions. However, so far only in rather exceptional circumstances, estimated at 2% of cases, a suspect is convicted on the basis of material gathered by applying covert investigative methods. Many of these are major cases involving very serious crimes. Also, the change in policy doesn't mean that any information or any piece of evidence obtained in such a way may be utilised as evidence in court. There are certain important limitations on this. A classic example is the situation in which person A was originally

the target person, but the application of the special investigative measures resulted also in obtaining material constituting proof that person B committed an offence. In one country materials gathered against B while tapping A could not be used as evidence in court. However, they could be used only as a ground to apply for warrant to use special investigative measures against B. The same applies to the other country. Such information on B would be considered as information requiring further investigation. The same applies to the situation when certain information were obtained from relations of the target person. For example, according to the case law, evidence on offences committed by A obtained from tapping conversations of his wife (on A′s telephone) could not be used in court as evidence. In one of the two countries there is also another important restriction to the use of intercepted material: it cannot be the only evidence. For a conviction, supplementary material evidence is needed.

In the third country under survey, the situation is a little bit different. Here, material gathered by intercepting communications transmitted on public telecommunications systems cannot be used as evidence in court, as the relevant law prohibits this. On the other hand, material obtained while using intrusive surveillance, obtained lawfully, may be used as evidence in court. If such methods produce also evidence against other persons, which were not considered to be suspects earlier, it may be also used as evidence in another case or (depending on circumstances) used to start a new investigation. The only one limitation on the evidentiary use of such material would be the character of the new offence, i.e. whether it is evidence of a serious offence which makes application of the intrusive surveillance possible at all.

The main reason for not disclosing intercepted material is protection of police tactics and investigative techniques. Also protection of informers as sources of information is considered highly important. However, the present system is not consistent. As said before, the results from intrusive surveillance can be presented as evidence during the trial. Also communication that was intercepted abroad can be used as such and this actually has happened several times. The present practice in this country of not revealing the use of interception to all members of the investigative team, only to those who really need to know, might lead to a less efficient performance of the team as a whole.

In general, special investigative methods can also be applied for international co-operation purposes, on the basis of existing agreements on mutual assistance in criminal matters. In one of the member States this leads to the peculiar situation that material from a public telecommunication system, that has been intercepted abroad in accordance with the laws of that country, can be used as evidence during a criminal trial, while the same sort of material intercepted in the country itself cannot. Concerning tracing and tracking across borders it is common practice that the authorities of the other country (or countries) involved are notified when use is made of a remote tracking device, e.g. attached to a suspicious vehicle or ship under surveillance. Surveillance teams do not cross national borders themselves. In some cases surveillance assistance is requested from the authorities on the other side of the border. This does not occur very often, partly because of the (expected) delay caused by long bureaucratic procedures.

Regarding the effectiveness of wiretapping and other covert investigative methods, there was general consensus among the people interviewed in the course of this best practice survey that in general, these methods are very helpful in the fight against organised crime. In many cases there

were virtually no other possibilities to gather (enough) evidence against the suspects or alternatives were generally disapproved as being too dangerous (e.g. the use of police infiltrators). However, in many cases, interception of communication and intrusive surveillance were combined with other, less intrusive, investigative techniques. This makes it very difficult to establish in a scientific manner the effectiveness of the use of covert methods. In many cases the intercepted material forms the basis for the questioning of arrested suspects. The fact that the police already knows a lot about the criminal activities of the group and the involvement of each of the members undoubtedly contributes to willingness of suspects to confess. In such a case, usually not the intercepted material but the confession is used as evidence in court. Because of this, it is not possible to estimate the number of convictions which were based primarily on information gathered by interception of communication or intrusive surveillance. However, it is clear that such material is very often used to direct the ongoing investigation. Furthermore, it is sometimes used to disturb the activities of criminal organisations. The representatives of the three countries, who were interviewed for this best practice survey, all shared the opinion that covert investigative methods are indispensable in the fight against organised criminals. A number of them even said that these methods gain significance, among other things in the pro-active tackling of corruption.

2.11 Related investigative methods

Since interception of communication and surveillance in private places are very intrusive methods of investigation, law enforcement officials consider the application of less intrusive measures first. As a consequence, they are used more often, especially in the first phase of an investigation. The two related methods that are used most frequently, at least in two of the three countries surveyed,[5] are the gathering of information on communications traffic[6] in which the target person is involved, and systematic "round-the-clock" surveillance on public places (either or not with the help of electronic devices). These methods are particularly useful in getting a comprehensive insight into the movements, lifestyle and personal network of a target person who is suspected of involvement in organised crime. Often, the (first) results of the application of these measures are used to get the necessary approval for the interception of communication for the target person and in some cases also for his/her apparent associates. The fact that many serious criminals nowadays are quite surveillance conscious and undertake various precautions, often makes the use of more intrusive methods necessary in order to gather enough evidence to bring a suspect to the court and get him or her convicted.

In two of the three countries in the survey, no judicial approval was necessary for the application of the two methods mentioned. In one member State, the public prosecutor has to approve the monitoring of communications traffic. In the other one, a senior police officer's decision is sufficient. In the third country a positive decision of a judge is needed for the gathering of information on communication traffic as well as for surveillance of suspects, even in public locations.

---

5 During the survey we did not get a good view on the situation regarding the use of these methods in the third member State.

6 This information usually includes data on the number calling or called (even if there is no successful connection established) and the beginning, end and duration of the connection.

Another frequently applied investigative method in all three member States is the use of informers. For this widely used method no judicial approval is needed in any of the three countries. Since this survey is concentrating on surveillance and interception of communication, the subject is not treated further here.

Sometimes intelligence or evidence is gathered by police officers who are working undercover and are "wired up" with a recording or transmitting device or who are filmed during conversations with a suspect. In two of the three countries surveyed, such use of undercover officers is regulated in the law and such recording of private speech is in principle allowed without judicial approval. However, in one of these countries, permission by a judge is needed for the recording of communication inside a private residence, even when a police officer is participating in the conversation. In the other member State the approval of a senior police officer suffices. The same rules apply to video recording in these circumstances.

Regarding the role of the undercover officer the three member States differ in their regulations. In general, deception of suspects seems to be allowed in all three countries, as long as suspects are not provoked or enticed to commit a crime that they would not otherwise have perpetrated. The question whether or not an undercover police officer can commit a crime himself, is answered differently in the three countries. However, it goes beyond the scope of this study to provide details on this specific issue.

A last investigative method to be discussed in this regard is the use of storefronts by law enforcement. Such firms can offer facilities for criminal groups, such as assistance in the laundering of criminal proceeds, the fencing of stolen goods or the transport or storage of illicit drugs. The difference between this method and the ones discussed before, is that storefronts need not to be set up in the course of a specific investigation but can offer facilities to the criminal fraternity in general. The method is sometimes criticised because of the risk of entrapping innocent people. In practice, in one of the three member States surveyed, the judiciary approved the running of a second-hand goods shop that pretended to be a "fencing" business. Even the posing of undercover officers as "contract killers" was accepted within certain restrictions, the most important one being that the defendant was not encited to commit an offence that he would not otherwise have committed. In another member State, the law explicitly allows the police to set a trap in order to expose the perpetrator of a criminal offence or to obtain evidence, as long as this does not cause injury or damage to health. The legal situation in the third country in the survey regarding this method is not clear, though in practice storefronts seem to be used by the police.

3. Conclusions and suggestions

3.1 Conclusions

In all three countries visited, organised crime has increased significantly in the past ten years. Governments consider organised crime to be a serious problem and give high priority to its repression.

Typical for the activities of organised crime groups is the circumstance that many individuals are involved, the illegal acts are perpetrated on different places and occur not at one

point in time but during a prolonged period of time. In many organised crime cases, e.g. in the trafficking of illicit narcotics, illicit arms or human beings, hardly any forensic evidence can be traced. Since these are "victimless" and often also "witness-less" crimes, such incidents are seldom reported to the police. Therefore, traditional investigative methods and techniques are not always fruitful. Law enforcement can detect and prosecute these types of crime effectively by making use of non-traditional investigative methods.

In the last five to ten years, governments in the member States visited have come to the conclusion that the combating of criminal organisations calls for new investigative methods, including covert methods like controlled deliveries, undercover policing and the interception of communication through the use of a great variety of modern technical means. In all three countries, organised crime has changed the face of criminal investigation. Many new laws concerning investigative methods and other measures to combat organised crime have come into force only recently. The implementation of new legal methods for the gathering of data is not seldom hampered and delayed by obstacles of technical and financial nature. The complexity of new legislation also leads to discussions within the law enforcement community on its interpretation and sometimes to a too restricted use in practice. As a result, in general the experience with covert investigative methods is still limited. Nevertheless, on the basis of the study visits in the three member States of the Council of Europe (and the literature gathered and studied), with some hesitations resulting from the lack of empirical data, we can conclude that in particular the interception of communication and intrusive surveillance seem to be quite effective in the combat against organised crime, especially in investigations directed towards international operating criminal groups, since they have to resort to telecommunication in order to organise their complex illicit activities. Law enforcement officials exploit this weakness of international criminal structures effectively by the interception of the communication (particularly telephone conversations) between the members of such groups.

However, the use of covert police methods is also associated with grave risks[7]. Law enforcement officials should carry out their duties in the combating of criminal organisations with minimum interference to the lives and liberties of individual citizens. A democratic society gives significant weight to fairness and rejects the notion that the end justifies the means. Therefore, the use of covert investigative methods requires greater justification than conventional police methods. Notions like the subsidiarity and proportionality principles and the risk of collateral collusion should be taken into consideration in the process of authorising the use of covert investigative methods. Elaborate legislative controls over and strict monitoring of covert operations by prosecutorial and judicial authorities are essential. In the countries that were visited during this best practice study, the above mentioned principles do play a role in the authorisation process of most, if not all, covert investigative methods. Furthermore, the control over the use of covert techniques is made possible by the recording of the investigative activities and the immediate availability of these records upon request for inspecting (judicial) authorities.

International criminal organisations increasingly use sophisticated communication techniques. They use a great variety of channels that make it easy to communicate across national

---

[7] For details see G.T. Marx: Undercover: Some implications for policy. C. Fijnaut & G.T. Marx (eds.): Undercover. Police surveillance in comparative perspective. Kluwer Law International, The Hague - London - Boston, 1995.

borders (including static and mobile phones, pagers, E-mail, etc.). The large number of (potential) communication channels already causes trouble for the interception by law enforcement. The use of encryption, which at the moment is observed in rare cases, in the near future will seriously hamper the possibilities to intercept the telecommunication between members of the more sophisticated and therefore in potential the most dangerous criminal groups.

3.2 Suggestions

1. Although the most important special investigative methods, interception of communication and intrusive surveillance, are applicable in all three member States surveyed, at the moment there are major differences in the types of crime for which covert investigative methods are allowed, the parameters which are to be taken into consideration in the authorisation procedure and the agencies which can decide on the authorisation.

2. Since one of the typical features of organised crime is its trans-national character, and covert investigative methods are in general, in comparison to traditional police methods, more effective in the fight against this type of crime, harmonisation of the relevant legal provisions is important. Covert investigative methods should in principle be applicable at least when there is probable cause for belief that one or more individuals are committing, have committed, or are about to commit an offence which is to be considered as organised crime. In the authorisation procedure, among other matters, it should be taken into consideration that normal investigative procedures have been attempted but have failed or appear unlikely to succeed. Furthermore, into consideration should be taken the probable cause for belief that particular communications will be obtained through the proposed interception or that specific proof will be obtained through the proposed intrusive surveillance.

3. In this best practice survey, several special investigative methods were encountered which were not described in a formal (statute) law. This raises questions on the legality of these methods. Examples are the systematic surveillance for a prolonged period of time of suspects moving in public places and the monitoring of communications traffic. These methods should be regarded as intrusions into the private life of the individuals involved and therefore should be regulated by law. Furthermore, they should be applied for pursuing legitimate purposes only and they should be necessary and proportional to that purpose.

4. For the safeguarding of civil liberties, governments should formulate and publish guidelines for all law enforcement bodies involved in covert investigative methods, which describe in clear language the ethical standards, authorisation procedures, record-keeping rules, complaints procedures and other guiding principles that law enforcement should apply while using such methods and their results.

5. Governments should make it a legal obligation for all telecommunication providers who operate in the country to establish the necessary technical facilities that allow interception of communications on behalf of the law enforcement bodies of that

country.

6. Governments should assist in the interception of telecommunication on, to, from or via their territory at the request of judicial authorities from other member States.

7. Governments should try and establish international standards for the encryption of telecommunication and promote law enforcement access to encrypted telecommunication as a legitimate regulatory requirement.

8. Governments should create a national reporting system on the use of special investigative techniques and publish annual reports, written by an independent high authority, on the use of such methods.

9. An application procedure which knows more than three levels, might unintentionally inhibit the legitimate use of interception of communication by law enforcement bodies. Excessive bureaucracy should be avoided or eliminated. In general, two (hierarchic levels within the) instances involved in the application procedure should suffice.

10. Although, in principle, the increasing co-operation between law enforcement bodies and national security services can be fruitful in the combating of criminal organisations, extra precautions should be taken to prevent the potential illegitimate gathering of criminal evidence by security services (who on the one hand have more powers than the police to use covert investigative techniques but on the other hand are more committed to the concealment of sources and methods and whose activities are neither authorised nor monitored by judicial authorities).

11. In general, the national laws should not prohibit the use of legitimately intercepted material (and other material that has been gathered through the use of covert investigative methods) as evidence in court. When applicable, the prosecutor should decide whether its use is needed in view of other available evidence and the importance of the case while remaining cautious as not to reveal covert techniques without necessity.

12. In the fight against organised crime, law enforcement officials should use methods like tracking (in combination with surveillance in public places) and the monitoring of communications traffic as much as possible, as they are less intrusive than the interception of conversations. Where appropriate, law enforcement should apply a combination of investigative methods to guarantee maximum results in a short period and to minimise (in time) the intrusion in the private life of the suspect as well as of individuals who belong to their environment. This tactic is also useful to overcome counter measures by criminal organisations (such as the use of coded communication and counter surveillance).

13. Law enforcement should be allowed to formulate applications/approvals for the interception of communication in a manner flexible enough to counteract the habit of some (especially experienced and organised) criminals to change devices frequently.

For this reason it is recommended that applications and approvals for the interception of communication specify the identity of the suspect(s) involved and leave room to the different types, channels, and specific communication devices which the target person(s) might use. However, an exception should be made for public telephone and other public communication devices. For the interception of communication via such devices an approval specifying the apparatus should be required.

14. Because of the potential infringement upon human rights, especially the right to lead a private life, the judiciary or another independent high authority should be authorised to exercise extensive *a priori* and *ex post facto* control on the use of covert investigative methods. At all times there should be a legal possibility either by the defence or by an independent authority (e.g. a judge) to check the legitimacy of the ways in which evidence was gathered.

15. National laws should oblige law enforcement bodies (or other authorities involved) to delete as soon as possible, but in any case within 10 days after its recording, any intercepted telecommunication between individuals none of whom are suspected of having committed or prepared a crime.

16. Persons who feel that their rights (might) have been violated through the use of covert investigative methods, should in general be able to seek redress before courts of law or other judicial bodies. These courts should have jurisdiction to determine whether such method(s) are or were applied in this case and whether this happened within the legal powers and functions of the law enforcement authority involved. The judicial body should have the right to determine whether there was undue harassment of the individual or abuse of discretionary powers in his or her regard. Should this be established by the judicial body, it should be able to apply appropriate sanctions.

17. The national laws that regulate the use of special investigative methods should not limit the number of extensions for interceptions and other measures; however, it should contain a provision which stipulates that a judge or another independent high authority should check the necessity of every extension in the light of - *inter alia* - the principles of subsidiarity and proportionality.

18. Governments should provide law enforcement with the necessary facilities to allow interception of telecommunication all over the country and not restricted to specific areas, channels or technical means (e.g. mobile phones).

19. Governments should make sure all of the intercepted communication is listened to by functionaries who are able and authorised to judge its relevance for the ongoing investigation.

20. Governments should make sure the quality and trustworthiness of interpreters involved in investigations against organised crime groups are guaranteed and checked regularly.

21. Governments should set preconditions in such a way that in cases of international organised crime, facilities for the simultaneous translation of intercepted conversation in a foreign language are readily available upon the request of the investigative team.

22. Law enforcement bodies should be obliged to store material that has been gathered by means of covert investigative methods in a safe place until the trial is completed or until the decision about non-prosecution of the subject(s) involved has a definite status. This gives the trial judge the opportunity to decide whether or not, and if so, what parts of, audio and video tapes that contain intercepted communication and other material collected should be disclosed to the defence.