COUNCIL OF EUROPE CONSEIL DE L'EUROPE

"SPECIAL INVESTIGATION TECHNIQUES" IN RELATION TO SERIOUS CRIMES INCLUDING ACTS OF TERRORISM

Recommendation Rec(2005)10

Adopted by the Committee of Ministers
of the Council of Europe
on 20 April 2005

and Explanatory Memorandum

This text is available on Internet: http://cm.coe.int
click "Documents", then "Texts adopted / Recommendations"

Legal issues

1. Recommendation Rec(2005)10, adopted by the Committee of Ministers of the Council of Europe on 20 April 2005, was prepared by the Committee of Experts on special investigation techniques (PC-TI), set up under the aegis of the European Committee on Crime Problems (CDPC).

2. This publication contains the text of Recommendation Rec(2005)10 and the explanatory memorandum related thereto.

COUNCIL OF EUROPE
COMMITTEE OF MINISTERS

Recommendation Rec(2005)10
of the Committee of Ministers to member states on
"special investigation techniques" in relation to serious crimes including acts of terrorism

(Adopted by the Committee of Ministers on 20 April 2005
at the 924th meeting of the Ministers' Deputies)

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

Recalling that the aim of the Council of Europe is to achieve a greater unity among its members;

Recalling that in Resolution No. 1 on combating international terrorism adopted at the 24th Conference of European Ministers of Justice (Moscow, 4-5 October 2001), the Committee of Ministers was invited to adopt urgently all normative measures considered necessary for assisting states to prevent, detect, prosecute and punish acts of terrorism;

Considering that the final report of the Multidisciplinary Group on International Action against Terrorism (GMT) and the subsequent decisions of the Committee of Ministers recognise the use of special investigation techniques as a priority area of the Council of Europe's legal action against terrorism;

Recalling that in Resolution No. 1 on combating terrorism, adopted at the 25th Conference of European Ministers of Justice (Sofia, 9-10 October 2003), the Committee of Ministers was invited, *inter alia*, to pursue without delay work with a view to adopting relevant international instruments on the use of special investigation techniques;

Bearing in mind the final report on special investigation techniques in relation to acts of terrorism prepared by the Committee of Experts on Special Investigation Techniques in relation to Acts of Terrorism (PC-TI) and the opinions of the Committee of Experts on Terrorism (CODEXTER) and of the European Committee on Crime Problems (CDPC) thereon;

Bearing in mind the surveys on "best practices" against organised crime carried out by the Group of Specialists on Criminal Law and Criminological Aspects of Organised Crime (PC-S-CO), as well as the reports adopted in the framework of the Council of Europe's technical cooperation programmes for the fight against corruption and organised crime;

Taking into account Recommendation No. R (96) 8 on crime policy in Europe in a time of change and Recommendation Rec(2001)11 concerning guiding principles in the fight against organised crime;

Taking into account the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108, 28 January 1981) and its Additional Protocol on Supervisory Authorities and Transborder Data Flows (ETS No. 181, 8 November 2001); Recommendation No. R (87) 15 regulating the use of personal data in the police sector; and Recommendation No. R (95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services;

Taking into account the existing Council of Europe conventions on cooperation in the penal field, as well as similar treaties which exist between Council of Europe member states and other states;

Mindful of the Guidelines on human rights and the fight against terrorism, adopted by the Committee of Ministers of the Council of Europe on 11 July 2002;

Mindful of the obligation on member states to maintain a fair balance between ensuring public safety through law enforcement measures and securing the rights of individuals, as enshrined in the provisions of the European Convention on Human Rights and the case-law of the European Court of Human Rights in particular;

Considering that special investigation techniques are numerous, varied and constantly evolving and that their common characteristics are their secret nature and the fact that their application could interfere with fundamental rights and freedoms;

Recognising that the use of special investigation techniques is a vital tool for the fight against the most serious forms of crime, including acts of terrorism;

Aware that the use of special investigation techniques in criminal investigations requires confidentiality and that any efforts to pursue the commission of serious crime, including acts of terrorism, should where appropriate be thwarted with secured covert means of operation;

Aware of the need to reinforce the effectiveness of special investigation techniques by developing common standards governing their proper use and the improvement of international cooperation in matters related to them;

Recognising that the development of such standards would contribute to further build public confidence as well as confidence amongst relevant competent authorities of the member states in the use of special investigation techniques,

Recommends that governments of member states:

i. be guided, when formulating their internal legislation and reviewing their criminal policy and practice, and when using special investigation techniques, by the principles and measures appended to this Recommendation;

ii. ensure that all the necessary publicity for these principles and measures is distributed to competent authorities involved in the use of special investigation techniques.

Appendix to Recommendation Rec(2005)10

Chapter I – Definitions and scope

For the purpose of this Recommendation, “special investigation techniques” means techniques applied by the competent authorities in the context of criminal investigations for the purpose of detecting and investigating serious crimes and suspects, aiming at gathering information in such a way as not to alert the target persons.

For the purpose of this Recommendation, “competent authorities” means judicial, prosecuting and investigating authorities involved in deciding, supervising or using special investigation techniques in accordance with national legislation.

Chapter II – Use of special investigation techniques at national level

a. General principles

1. Member states should, in accordance with the requirements of the European Convention on Human Rights (ETS No. 5), define in their national legislation the circumstances in which, and the conditions under which, the competent authorities are empowered to resort to the use of special investigation techniques.

2. Member states should take appropriate legislative measures to allow, in accordance with paragraph 1, the use of special investigation techniques with a view to making them available to their competent authorities to the extent that this is necessary in a democratic society and is considered appropriate for efficient criminal investigation and prosecution.

3. Member states should take appropriate legislative measures to ensure adequate control of the implementation of special investigation techniques by judicial authorities or other independent bodies through prior authorisation, supervision during the investigation or ex post facto review.

b. Conditions of use

4. Special investigation techniques should only be used where there is sufficient reason to believe that a serious crime has been committed or prepared, or is being prepared, by one or more particular persons or an as-yet-unidentified individual or group of individuals.

5. Proportionality between the effects of the use of special investigation techniques and the objective that has been identified should be ensured. In this respect, when deciding on their use, an evaluation in the light of the seriousness of the offence and taking account of the intrusive nature of the specific special investigation technique used should be made.

6. Member states should ensure that competent authorities apply less intrusive investigation methods than special investigation techniques if such methods enable the offence to be detected, prevented or prosecuted with adequate effectiveness.

7. Member states should, in principle, take appropriate legislative measures to permit the production of evidence gained from the use of special investigation techniques before courts. Procedural rules governing the production and admissibility of such evidence shall safeguard the rights of the accused to a fair trial.

c. Operational guidelines

8. Member states should provide the competent authorities with the required technology, human and financial resources with a view to facilitating the use of special investigation techniques.

9. Member states should ensure that, with respect to those special investigation techniques involving technical equipment, laws and procedures take account of the new technologies. For this purpose, they should work closely with the private sector to obtain their assistance in order to ensure the most effective use of existing technologies used in special investigation techniques and to maintain effectiveness in the use of new technologies.

10. Member states should ensure, to an appropriate extent, retention and preservation of traffic and location data by communication companies, such as telephone and Internet service providers, in accordance with national legislation and international instruments, especially the European Convention on Human Rights and the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108).

11. Member states should take appropriate measures to ensure that the technology required for special investigation techniques, in particular with respect to interception of communications, meets minimum requirements of confidentiality, integrity and availability.

d. Training and coordination

12. Member states should ensure adequate training of competent authorities in charge of deciding to use, supervising and using special investigation techniques. Such training should comprise training on technical and operational aspects of special investigation techniques, training on criminal procedural legislation in connection with them and relevant training in human rights.

13. Member states should consider the provision of specialised advice at national level with a view to assisting or advising competent authorities in the use of special investigation techniques.

Chapter III – International cooperation

14. Member states should make use to the greatest extent possible of existing international arrangements for judicial or police cooperation in relation to the use of special investigation techniques. Where appropriate member states should also identify and develop additional arrangements for such cooperation.

15. Member states are encouraged to sign, to ratify and to implement existing conventions or instruments in the field of international cooperation in criminal matters in areas such as exchange of information, controlled delivery, covert investigations, joint investigation teams, cross-border operations and training.

Relevant instruments include, *inter alia*:

– the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances of 20 December 1988;
– the Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime of 8 November 1990 (ETS No. 141);
– the Criminal Law Convention on Corruption of 27 January 1999 (ETS No. 173);
– the Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters of 8 November 2001 (ETS No. 182);
– the Convention on Cybercrime of 23 November 2001 (ETS No. 185);
– the United Nations Convention against Transnational Organised Crime of 15 November 2000 and the Protocols thereto;
– the United Nations Convention on Corruption of 31 October 2003.

16. Member states are encouraged to make better use of existing relevant international bodies, such as the Council of Europe, the European Judicial Network, Europol, Eurojust, the International Criminal Police Organisation (Interpol) and the International Criminal Court, with a view to exchanging experience, further improving international cooperation and conducting best practice analysis in the use of special investigation techniques.

17. Member states should encourage their competent authorities to make better use of their international networks of contacts in order to exchange information on national regulations and operational experience with a view to facilitating the use of special investigation techniques in an international context. If needed, new networks should be developed.

18. Member states should promote compliance of technical equipment with internationally agreed standards with a view to overcoming technical obstacles in the use of special investigation techniques in an international context, including those connected with interceptions of mobile telecommunications.

19. Member states are encouraged to take appropriate measures to promote confidence between their respective competent authorities in charge of deciding to use, supervising or using special investigation techniques with a view to improving their efficiency in an international context, while ensuring full respect for human rights.

Introduction

1. At its 109th session on 8 November 2001, in the wake of the terrorist attacks on the United States of America on 11 September 2001, the Committee of Ministers of the Council of Europe "agreed to take steps rapidly to increase the effectiveness of the existing international instruments within the Council of Europe on the fight against terrorism, by, *inter alia*, setting up a Multidisciplinary Group on International Action against Terrorism [GMT]".

2. The tasks of the GMT included identifying appropriate measures that could be taken in the fight against terrorism and preparing a report for the Committee of Ministers, including additional actions that the Council of Europe could implement in order to contribute to the international fight against terrorism.

3. In its final activity report, submitted to the Committee of Ministers at its 111th session in November 2002, the GMT set out a number of priority areas for action that the Council of Europe could begin to implement in 2003. Those priorities included special investigation techniques.

4. The GMT considered that, owing to its complex and secret nature, as well as the technical nature of the area concerned, the investigation of terrorist activities raised serious difficulties. It recalled that these difficulties were accentuated by the frequent links between terrorism and other forms of crime (e.g. money laundering, drug trafficking, illegal arms sales, organised crime, etc) and by the difficult distinction between legal and illegal activities. The often complex nature of important terrorist actions and therefore of investigations has led to the awareness that these matters can only be effectively and rapidly addressed by making use of special working methods (e.g. undercover agents, electronic surveillance, multidisciplinary approaches and inter-service co-operation). However, the GMT insisted on the fact that, in doing so, it was essential to ensure that human rights guarantees, as enshrined in relevant international legal instruments, were fully respected.

5. For this reason, the GMT recommended to the Committee of Ministers that it be given the task of examining, in co-operation with the European Committee on Crime Problems (CDPC), the issues above with a view to developing, where necessary, guidelines to facilitate and increase the effectiveness of pre-trial investigation in cases of terrorism, bearing in mind human rights guarantees.

6. The Committee of Ministers endorsed the proposals made by the GMT. Accordingly at its 828th meeting (Strasbourg, 13 February 2003), the Committee of Ministers at Deputies' level, following the request by the European Committee on Crime Problems (CDPC), adopted specific terms of reference for a Committee of Experts on Special Investigations Techniques in relation to Acts of Terrorism (PC-TI).

7. According to these terms of reference, the PC-TI was requested "to study the use of special investigation techniques respective of European criminal justice and human rights standards, with a view to facilitating the prosecution of terrorist offences and increasing the effectiveness of law enforcement, and to make proposals as to the feasibility of preparing an appropriate instrument in this field".

8. The Committee was composed of over thirty national experts from Council of Europe member and observer states. It was also composed of representatives from the European Commission and the Secretariat General of the Council of the European Union, as well as representatives of the Steering Committee for Human Rights (CDDH) and of the European Committee on Legal Co-operation (CDCJ). The Committee met three times in 2003: the first meeting was held from 14 to 16 April, the second from 2 to 4 July and the third from 22 to 24 September.[1]

9. In its final report, the PC-TI concluded that it would be feasible to draw up a recommendation on the use of special investigation techniques, so as to invite member states to develop common principles governing the use of special investigation techniques reconciling the effectiveness of the fight against serious crime, such as terrorism, with the respect of human rights and the fundamental principles of penal justice. The recommendation should furthermore invite member states to identify best practice with respect to the role of the judicial and law

[1] Reports of these meetings (docs PC-TI (2003) 6, 10 and 12) are accessible on the PC-TI website (www.coe.int/gmt, then click on PC-TI).

enforcement authorities involved in the use of SIT and improve international cooperation in relation with the use SIT.

10. At their 25th Conference, the European Ministers of Justice welcomed these conclusions, which were subsequently endorsed by the Committee of Experts on Terrorism (CODEXTER) at its first meeting (27-30 October 2003). The CODEXTER advocated the preparation of international instruments on special investigation techniques, emphasising that the adoption of such instruments would enhance the efficiency of the fight against terrorism. The Committee of Ministers took note of these conclusions at its 864th meeting (4 December 2003).

11. At its plenary meeting in March 2004, the European Committee on Crime Problems (CDPC) approved revised draft specific terms of reference for a new Committee of Experts on Special Investigation Techniques (PC-TI) and submitted them to the Committee of Ministers, which adopted them at its 884th meeting (19 May 2004).

12. Pursuant to its new specific terms of reference, the PC-TI was, on the basis of the conclusions of the final report by the former Committee of Experts on Special Investigation Techniques in relation to Acts of Terrorism, and with a view to developing common principles governing the use of special investigation techniques and of improving international co-operation in matters related to the use of special investigation techniques, including in relation to acts of terrorism, called upon:

- as a matter of priority to draw up a recommendation taking into account the relevant international instruments already adopted, in particular within the Council of Europe;

- where appropriate, and upon request, to advise other Council of Europe Committees on the development of standards aiming to improve the conventional framework in this field.

13. In accordance with its specific terms of reference, the PC-TI started its work in October 2004 and completed it in February 2005, having held three plenary meetings during this period.

14. At its last meeting, the PC-TI adopted the draft recommendation and took note of the draft explanatory memorandum relating thereto, which were transmitted to the CDPC for its approval. The draft recommendation was approved by the CDPC in March 2005 and adopted by the Committee of Ministers of the Council of Europe on 20 April 2005.

General Considerations

15. The aim of this recommendation is to promote the effective use of SIT by the competent authorities in the framework of criminal investigations in relation to serious crimes, including acts of terrorism, whilst ensuring strict respect for the rights and freedoms of the individual. To this end, the recommendation, firstly, recalls or provides for some common principles that should be respected when Member states are regulating SIT and when they are used by their competent authorities (Chapter II). Secondly, the recommendation suggests measures to be taken with a view to improving co-operation between member states in matters related to them (Chapter III).

16. It should be recalled that several instruments of the Council of Europe already deal with the question of SIT such as, for instance, the Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (Article 4 - ETS No 141), the Criminal Law Convention on Corruption (Article 23 - ETS No. 173), the Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters (Articles 17 to 20 – ETS No 182), or the Committee of Ministers' Recommendation Rec(2001)21 on the fight against organised crime. However, these instruments address issues connected with the use of SIT only in so far as these are being used in relation to their respective scope while the present text offers a comprehensive approach to the use of SIT in connection with all forms of serious crimes, including acts of terrorism.

17. SIT are particular techniques because of their secret nature (see hereunder, para. 27). It is because of their secret nature that they are considered a vital tool in the fight against serious crimes, including acts of terrorism. On the other hand, their use may interfere with fundamental rights and freedoms, such as the right to respect for private life or the right to a fair trial. Therefore, the recommendation seeks to strike a balance between the need to enhance the efficiency of the fight against serious crimes, including acts of terrorism, by promoting the use of SIT, and the need to ensure the protection of fundamental rights and freedoms.

18. The search for a balance is inspired by a similar approach adopted by the European Court of Human Rights. The Court found that: "Democratic societies nowadays find themselves threatened by highly sophisticated forms of espionage and by terrorism, with the result that the State must be able, in order effectively to counter such threats, to undertake the secret surveillance of subversive elements operating within its jurisdiction. The Court has therefore to accept that the existence of some legislation granting powers of secret surveillance over the mail, post and telecommunications is, under exceptional conditions, necessary in a democratic society in the interests of national security and/or for the prevention of disorder or crime". "Nevertheless, the Court stresses that this does not mean that the Contracting States enjoy an unlimited discretion to subject persons within their jurisdiction to secret surveillance. The Court, being aware of the danger such a law poses of undermining or even destroying democracy on the ground of defending it, affirms that the Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate. The Court must be satisfied that, whatever system of surveillance is adopted, there exist adequate and effective guarantees against abuse. This assessment has only a relative character: it depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering such measures, the authorities competent to permit, carry out and supervise such measures, and the kind of remedy provided by the national law."[2]

19. The recommendation addresses the use of SIT in connection with not only terrorism but, more generally, with serious crimes, including acts of terrorism. Indeed, the Committee of Experts on Special Investigation Techniques concluded that the principles laid down in the recommendation should not be specifically confined to the fight against terrorism but that they are applicable in the more general context of combating serious crimes. The Committee did not find it necessary to define the term "serious crimes" but instead found that, for the purposes of the Recommendation, it was more appropriate to leave member states a margin of appreciation in setting thresholds for qualifying the gravity of the crimes. Article 2 (b) of the UN Convention against Transnational Organised Crime, which provides for a definition whereby ""Serious crime" shall mean conduct constituting an offence punishable by a maximum deprivation of liberty of at least four years or a more serious penalty", can however serve as an indicator for those states that wish to define this notion more precisely. In any event, the term "serious crimes" covers acts of terrorism and organised crime offences.

Commentary on the provisions of the Recommendation

Preamble.

20. In the 7th paragraph, reference is made to best practice surveys carried out by the Committee of Experts on Criminal Law and Criminological Aspects of Organised Crime (PC-CO) and by the Group of Specialists on Criminal Law and Criminological Aspects of Organised Crime (PC-S-CO). The PC-CO was established in 1997 with a view to analysing the organised crime situation, assessing the counter-measures adopted, and identifying means of improving the effectiveness of both national response and international cooperation in this field. From 2000 to the end of 2003, the work of this Committee was continued by the PC-S-CO. The Committee and the Group of Specialists decided to carry out a series of best practice surveys. The purpose of these surveys was fairly simple: as certain European countries had developed innovative solutions to the problem of organised crime, it seemed appropriate and important to ensure that these be shared with other countries. The aim of the surveys was thus to document such experience in a limited number of countries and to disseminate the results in order to encourage and motivate relevant authorities throughout Europe. These surveys are accessible on the website of the Council of Europe. [3]

[2] ECHR, 6 September 1978, Klass and Others v. Germany, para. 48-50.

[3] http://www.coe.int/T/E/Legal_affairs/Legal_cooperation/Combating_economic_crime/Organised_crime/Documents/2Best_Practices_Survey.asp#TopOfPage.

21. Reference is also made in this paragraph to the Council of Europe's technical operation programmes for the fight against corruption and organised crime. Examples of such programmes include the Joint Programme between the European Commission and the Council of Europe on the Fight against Corruption and Organised Crime in States in Transition (Octopus II, 1999-2001) and the Programme against Corruption and Organised Crime in South-eastern Europe (PACO, since 1999).

22. With regard to the 9th paragraph, it should be noted that, in drawing up the recommendation, consideration has also been given to reports prepared by the Project Group on Data Protection (CJ-PD), and subsequently adopted by the European Committee on Legal Cooperation (CDCJ): see in particular the Report on the impact of data protection principles on judicial data in criminal matters including in the framework of judicial co-operation in criminal matters (adopted at the 74th meeting of CDCJ, 4-8 December 2000) and the Report containing guiding principles for the protection of individuals with regard to the collection and processing of data by means of video surveillance (adopted at the 78th meeting of CDCJ, 20–23 May 2003).

23. In the 12th paragraph, the reference to the European Convention on Human Rights and to the case-law of the European Court of Human Rights is aimed in particular at underlining the specific relevance of Articles 6, 8 and 13 in the context of the use of SIT.

24. In the part of the sentence that reads "common standards governing the proper use of SIT" in paragraph 16th, the terms "proper use" refers in particular to the use of SIT in conformity with human rights standards.

Paragraph ii:

25. The "competent authorities involved in the use of SIT" are, in accordance with "Chapter I. Definitions and scope", the judicial, prosecuting and investigating authorities involved in deciding, supervising or using SIT in accordance with national legislation.

Chapter I. Definitions and Scope

26. According to Chapter I, SIT are techniques applied by the competent authorities in the context of criminal investigations. The consequences of this are twofold: firstly, it means that the use of SIT in a different context, such as national security, does not fall within the scope of the recommendation; secondly, it leads to the fact that SIT that are being used in the context of criminal investigations are covered by the recommendation regardless of the title or identity of the authorities that have been involved in deciding, supervising or using SIT.

27. The first paragraph of this Chapter specifies that SIT are techniques used "in such a way as not to alert the target persons". The use of SIT would be superfluous, and might even be counterproductive, if the target persons were aware about the fact that such techniques are being used with a view to collecting information on their actions or activities. Consequently, SIT are often of a secret nature. "Secrecy" is present where an attempt is made to conceal what is being done. The aim of secrecy is not to alter the behaviour of the presumed offender but to deprive him or her of information.

For the purpose of this recommendation, SIT may include for instance: undercover operations (including covert investigations); front store operations (e.g. undercover company); informants; controlled delivery; observation (including cross-border observation); electronic surveillance; interception of communications (telephone, fax, e-mail, mail); searches (including of premises and objects, such as computers, cars, etc); cross-border (hot) pursuits; pseudo-purchases or other "pseudo-offences" as they are defined in national laws.

Chapter II. Use of SIT at national level

a) General Principles:

Paragraph 1:

28. The requirements laid down in this paragraph must be seen in particular in the context of the protection offered by Article 8 of the European Convention on Human Rights (ECHR) to the right to respect for private and

family life. Article 8 provides that: “Everyone has the right to respect for his private and family life, his home and his correspondence. 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.”

29. When regulating or using SIT, national authorities need to bear in mind that the use of SIT may affect not only the rights of the person who is suspected of having committed or prepared the offence, but also, directly or indirectly, the rights of other persons. In this respect, the appropriateness of a specific SIT may, *inter alia*, depend on the intrusiveness into the rights of other persons.

Besides, in order to ensure that the rights of such other persons are fully respected, member states could establish, if necessary, additional specific protection mechanisms (such as a “Commissioner for legal protection”).

30. When there is interference with an individual’s right to respect for his or her private life, it must be ensured, in particular, that such interference is justified under Article 8(2). This is to say that the interference must be (i) “in accordance with the law”, (ii) necessary in a democratic society and (iii) in pursuance of one of the legitimate aims set out in Article 8(2). Paragraph 1 should be read in conjunction with the first condition (point (i)) as it calls for a legal basis to be provided in domestic law for the use of any SIT.

31. It should be recalled that, in order to satisfy the requirements of the European Convention on Human Rights, domestic law must be sufficiently “precise” and “accessible” for an individual to be able to foresee with a reasonable degree of certainty the consequences of his or her actions, or the circumstances in which and the conditions on which authorities may take certain steps. In this regard, the European Court of Human Rights stated:

> "Firstly, the law must be adequately accessible: the citizen must be able to have an indication that is adequate in the circumstances of the legal rules applicable to a given case. Secondly, a norm cannot be regarded as 'law' unless it is formulated with sufficient precision to enable the citizen to regulate his conduct: he must be able – if need be with appropriate advice - to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail." [4]

32. As regards more specifically telephone tapping, the law should at least set out the categories of persons whose telephones may be tapped, the nature of the offences justifying the use of tapping, the duration of the measure, the procedure for drawing up the summary reports containing intercepted conversations, the precautions to be taken in order to communicate the recordings intact and in their entirety for possible inspection by the judge and the defence, and the circumstances in which they are to be erased or destroyed (in particular following discharge or acquittal of the accused).[5]

33. More generally, with regard to the compatibility of SIT with the requirements of Article 8, the Court has been called upon to examine a certain number of situations such as:

- With respect to telephone tapping:

34. The Court has laid down the principle that telephone tapping must comply with the law, considering that, where it does not, it is prohibited, regardless of whether it is for judicial purposes or for reasons of national security.[6]

- With respect to searches:

35. Depending on the scope of the measures and the guarantees provided by domestic law, to allow a non-judicial authority alone to decide on such operations[7] may constitute a violation of the Convention.

---

[4] ECHR, 26 April 1979, Sunday Times v. United Kingdom, p. 31, para. 49.
[5] ECHR, 24 April 1990, Huvig and Kruslin v. France; see also ECHR, 19 March 2002, Greuter v. The Netherlands, with respect to the proportionality test.
[6] ECHR, 27 November 1993, A. v. France.

36. In some circumstances, the Convention requires a judicial authority to decide on the appropriateness, number, duration and scope of search operations and for searches to be carried out within the limits of a warrant issued by a judge.[8] In other circumstances, the Court has accepted as lawful a purely administrative search in view of the strict legal framework in which it took place and the proportionate scope of the action.[9]

- With respect to interception of mail:

37. The Court has accepted that the existence of legislative provisions granting powers for the covert surveillance of correspondence and other items sent through the mail might be necessary as part of the fight against terrorism,[10] if appropriate and sufficient safeguards against abuse are provided. The Court's appreciation will depend upon the nature, extent and duration of any measures, the reasons required for ordering them, the authorities competent to authorise them, carry them out and review them, and the type of remedy provided for in domestic law.[11] Further protection is granted with respect to correspondence with a lawyer since this type of interference affects the rights of the defence.[12]

38. Electronic correspondence has introduced a new situation: where investigation of criminal offences or the protection of public order are legitimate reasons for interference, a clearly defined legal framework is required. The particularity of such interference is that it affects not only the secrecy of correspondence (information) but also the secrecy of communications (telephone lines) and the right to privacy at home (entering the hard disk of a computer installed in a home).

- With respect to photographing and filming:

39. The Court has accepted the legitimacy of such techniques in the very particular context of the fight against terrorism and during questioning by the security forces.[13] It stressed that this context influenced its assessment of the fair balance between the rights of the individual and the needs of society. However, it is clear that there must be a legal framework whose application is foreseeable, a legitimate aim, and that such techniques must be regarded as having been necessary in a democratic society for the prevention of crime.

- With respect to the use of informants:

40. The Court has accepted that the needs of police action may require the use of informants without that being in violation of Article 8 of the ECHR.[14] The police does not have a duty as such to reveal the identity of persons who provide them with information, but the using of such information as evidence before a tribunal will have to respect the right to a fair hearing guaranteed under Article 6 of the ECHR.

Paragraph 2:

41. Any legislative measure to allow the use of SIT needs to fulfil the requirement laid down in Paragraph 1. The extent to which SIT can be used depends on the degree to which such use is necessary and proportionate in a democratic society according to Article 8 of the ECHR and to the case-law of the European Court of Human Rights.[15] However, Paragraph 2 should not be interpreted as an obligation on member states to introduce additional SIT. The SIT that should be available depend on what is considered appropriate by national legislative authorities.

---

[7] ECHR, 25 February 1993, Funke, Crémieux and Miailhe v. France.
[8] ECHR, 15 July 2003, Ernst and Others v. Belgium.
[9] ECHR, 16 December 1997, Camenzind v. Switzerland.
[10] ECHR, Klass and Others v. Germany, op.cit.
[11] ECHR, 26 March 1987, Leander v. Sweden; ECHR, 2 August 1984, Malone v. the United Kingdom; ECHR, 25 June 1997, Halford v. the United Kingdom; ECHR, 12 Mai 2000, Kahn v. United Kingdom.
[12] ECHR, 28 June 1988, Schönenberger and Durmaz v. Switzerland.
[13] ECHR, 28 October 1994, Murray and Others v. the United Kingdom.
[14] ECHR, 30 August 1990, Fox, Campbell and Hartley v. the United Kingdom.
[15] ECHR, 16 December 1997, Cammenzind v/ Switzerland; ECHR, 27 June 2002, Butler v/ United Kingdom.

Paragraph 3:

42. Amongst the various types of control envisaged in this paragraph, the Committee of Experts on Special Investigation Techniques (PC-TI) considered that the most effective control would be a system of prior authorisation, although it would not always be appropriate to establish such a control.

43. The various types of control may be complementary, depending on the degree of intrusiveness in the private sphere occasioned by the use of SIT. For example, in undercover operations, there may be control at the beginning, during and at the end of the operation. At the beginning, the launching of the operation would be subject to there being sufficient reasons or suspicions; during the operation, regular reports would be made and, lastly, a precise description of the conduct of the operation would enable ex post facto control.

b) Conditions of use:

Paragraph 4:

44. With regard to the terms "sufficient reasons to believe", the difficulty in determining what is meant by "sufficient reasons" should not be underestimated. The essentially factual nature of the concept makes a legal definition of it almost impossible. As a source of inspiration to clarify the concept, one could refer to the interpretation given by the European Court of Human Rights with respect to the concept of "reasonable suspicion" within the meaning of Article 5 of the ECHR. In this context, the Court found that "having a 'reasonable suspicion' presupposes the existence of facts or information which would satisfy an objective observer that the person concerned may have committed the offence. What may be regarded as 'reasonable' will however depend upon all the circumstances".[16]

45. The reference to a crime "being prepared" covers situations where, although no offence has been committed, a person acted or is acting in a way that could objectively be considered as contributing to the preparation of an offence.

Paragraph 4 does not preclude the use of SIT, in accordance with the principles laid down in this recommendation, for ordinary crimes if necessary.

Paragraph 6:

46. This paragraph encourages competent authorities to apply other investigation methods than SIT if such methods enable the offence to be detected, prevented or prosecuted "with adequate effectiveness". The words "with adequate effectiveness" indicate that other investigation methods than SIT should be used if, firstly, they are capable of leading to the same results and, secondly, their implementation does not give rise to significant practical obstacles.

Paragraph 7:

47. The first sentence of the paragraph does not mean that SIT should exclusively be used to obtain information and material that can serve as evidence before the courts. It aims at ensuring that, where appropriate, information or material gained from the use of SIT can lawfully be produced in the course of a trial before national courts and calls on members states to enact appropriate legislation to this end.

48. As indicated in the second sentence of the paragraph, evidence gained from the use of SIT should not be submitted in such a way as to jeopardise the right of the accused to a fair trial, guaranteed by Article 6 of the ECHR. In this regard, it should be recalled that, even though Article 6 of the Convention "does not lay down any rules on the admissibility of evidence as such, which is therefore primarily a matter for regulation under national law",[17] the Convention requires the proceedings as a whole, including the way in which evidence is submitted, to be fair. In this context, it should be underlined that Paragraph 7 does not prevent member states from excluding

[16] ECHR, Fox, Campbell and Hartley v. the United Kingdom, op cit, para. 32.
[17] ECHR, 24 June 1988, Schenk v. Switzerland, para. 46.

the admissibility as evidence of information or material gained by SIT in extraordinary cases, in particular where the SIT has not been used in accordance with national law.

49. In the Lüdi and Teixera de Castro cases,[18] the Court considered that supervised operations and controlled operations were compatible with the rights of the accused only if those operations were conducted in the framework of a judicial investigation and the identity and role of the infiltrated officer were known to the judge. Conversely, action taken without judicial supervision would be unfair and would taint the procedure from the outset.

50. While the Court accepts the use of infiltrated officers whose role is not entirely passive,[19] it condemns provocation to commit offences.[20] There is provocation where the behaviour of the authorities has been decisive in the commission of an offence. The Court also considers that a conviction based substantially on the testimony of "agents provocateurs" violates the right to a fair hearing.

51. The use of undercover agents, anonymous informants and anonymous witnesses gives rise to particular legal concerns. The Court has often stated that the Convention does not prohibit the use of anonymous informants during a preliminary investigation but that the use of information thus obtained at the trial presents a problem with respect to fairness.[21] The Court takes as its starting-point the principle that evidence must be presented at the trial and debated in the presence of both parties; this does not, however, prohibit the use at the trial of statements made during the investigation, provided that those who made them have been cross-examined by the defence prior to the trial. The use of anonymous testimony by witnesses who do not appear at the trial for security reasons and whose identity remains unknown to the defence, and sometimes even to the trial judge, has to be examined. The admissibility of anonymous testimony depends on the circumstances of the case and on the answer to three questions emerging from the case-law: Is anonymity justified by a compelling reason? Have the resulting limitations on the effective exercise of the rights of the defence been adequately compensated for? Was the conviction exclusively or substantially based on such anonymous testimony?[22]

c) Operational guidelines:

Paragraph 10:

52. The retention and the preservation of traffic and location data may be necessary in any investigation into serious crime, including acts of terrorism. For the purpose of this Recommendation, it should be recalled that traffic data has been defined in Article 1, d) of the Convention on Cybercrime of 23 November 2001 (ETS No. 185) and in Article 2, b) of EC Directive 2002/58/EC. Location data has been defined in Article 2, c) of EC Directive 2002/58/EC.

53. Paragraph 10 calls for traffic and location data to be retained and preserved in accordance with "national legislation and international instruments, especially the European Convention on Human Rights and the Convention for the protection of individuals with regard to automatic processing of personal data (ETS No 108)".

54. However, Paragraph 10 should not be read or interpreted in a way that imposes any obligation on member states to introduce legislation on retention and preservation of traffic and location data that goes beyond obligations that already exist under international or national law.

The European Court of Human Rights does not appear to have had the opportunity to deal specifically with the problem of retention and preservation of traffic and location data. It seems however that such data could be considered as personal data. Indeed, in a judgment of 16 February 2000, the Court held that the collection by security services of data on a specific individual constituted an interference with the right to private life, even though those data had been collected without SIT being used.[23] A fortiori, the collection of personal data through

[18] ECHR, 15 June 1992, Lüdi v. Switzerland; ECHR, 9 June 1988, Teixeira de Castro v. Portugal.
[19] ECHR, Lüdi v. Switzerland, op. cit.
[20] ECHR, Teixeira de Castro v. Portugal, op. cit.
[21] ECHR, 20 November 1989, Kostovski v. the Netherlands.
[22] ECHR, Kostovski v. The Netherlands, op.cit.; ECHR, 23 April 1997, Van Mechelen v. The Netherlands; ECHR, 26 March 1996, Doorson v. The Netherlands.
[23] ECHR, 16 February 2000, Amann v. Switzerland.

the use of SIT would seem also to constitute an interference with the rights guaranteed under Article 8 which could only be admissible in so far as it is prescribed by law, necessary and proportionate.

Paragraph 11:

55. Interception of communications is one of the most commonly used SIT in member states. Paragraph 6 calls for such interception to meet "minimum requirements of confidentiality, integrity and availability". These requirements mean that the information should be accessible only to certain authorized persons (confidentiality), that the information should be authentic and complete, thus granting a minimum standard of reliability (integrity) and that the technical system in place to intercept telecommunications is accessible whenever necessary (availability).

Chapter III. International co-operation

Paragraph 14:

56. The terms "international arrangements" in this paragraph include not only multilateral but also bilateral agreements and instruments.

Paragraph 16:

57. The reference to the "Council of Europe" that appears in this paragraph, aims at inviting member states to increase their participation in the various existing or future committees of experts set up by the Committee of Ministers, as well as in any future European conferences or meetings to be organised by the Council of Europe in connection with the use of SIT.

58. The International Criminal Court (ICC) investigating and prosecuting activities can also contribute to the improvement of international co-operation. Over the last ten years, the United Nations ad hoc Tribunals (ICTY and ICTR) have gained valuable experience in using SIT in co-operation with relevant states and organisations. Examples of further relevant experiences might also be drawn from the activities of other international criminal justice mechanisms already in place (such as the Special Court for Sierra Leone, in particular the Serious Crimes Unit (SCU), or the Special Panel for Serious Crimes at the Dili District Court in Timor Leste) or soon to be activated (such as the War Crimes Chamber at Sarajevo or the Special Tribunal for Cambodia).

Paragraph 17:

59. This paragraph is based on the idea that member states should overcome the practical problems which hamper effective co-operation by reinforcing exchanges at the operational level between competent authorities.

Examples of such "practical problems" include those related to working procedures, including undue delays, lack of information, lack of language knowledge, undue bureaucracy, slow transmission of information, inappropriate point of contact, cost related issues and any other relevant technical issues.

This paragraph does not preclude authorities others than "competent authorities" in the meaning of this recommendation to exchange information on national regulations and operational experiences in the use of SIT.

Paragraph 18:

60. This paragraph is based on the idea that common technical references in the field of SIT should ease international co-operation. As far as "internationally agreed standards" is concerned, particular attention could be given to the work conducted by the European Telecommunications Standards Institute (ETSI) on this issue.[24]

[24] For more info: http://portal.etsi.org/li/Summary.asp and www.etsi.org.

Paragraph 19:

61. This paragraph is based on the idea that international co-operation between member states' competent authorities would be improved if there was a firm confidence in the conditions of use of SIT.

62. "Measures to promote confidence" could include participation of competent authorities in activities to be organised in the context of existing relevant international bodies referred in paragraph 16 or at the level of the networks of contacts referred in paragraph 17. It could also include common training.