COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 17 November 2016

CODEXTER (2016) 5 rev3

COMMITTEE OF EXPERTS ON TERRORISM

(CODEXTER)

UPDATING OF RECOMMENDATION REC(2005)10

Draft Recommendation of the Committee of Ministers to member States on "special investigation techniques" in relation to serious crimes including acts of terrorism

_____

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

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

3. Bearing in mind 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;

4. Taking into account the Opinion on the Protection of Human Rights in Emergency Situations (17-18 March 2006); the Report on the Democratic oversight of the Security Services (1-2 June 2007); and, the Report on Counter-Terrorism Measures and Human Rights (Venice, 4 June 2010) adopted by the European Commission for Democracy through Law (Venice Commission);

5. Recalling that the International Conference on The Use of Special Investigation Techniques to Combat Terrorism and Other Forms of Serious Crime (Strasbourg, 14–15 May 2013) acknowledged the need for updating the standards and guidelines applicable to the use of special investigation techniques;

6. Considering that the final report of the Committee of Experts on Terrorism (CODEXTER) adopted at the 25th Plenary Meeting (Istanbul, 23–24 October 2013) recognised the use of special investigation techniques as a priority area of the Council of Europe's legal action against terrorism;

7. Bearing in mind the sets of actions identified by the European Committee on Crime Problems (CDPC) in the White Paper on Transnational Organised Crime (Strasbourg, 6 October 2014) with regard to the fight against transnational organised crime and the use of special investigation techniques, 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;

8. Recalling that under the Action Plan on the fight against violent extremism and radicalisation leading to terrorism adopted at the 125th Session of the Committee of Ministers (Brussels, 19 May 2015), the Council of Europe was called upon to develop targeted activities capable of reinforcing the legal framework against terrorism and violent extremism and preventing and fighting violent radicalisation, while respecting human rights and the rule of law;

9. 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; Recommendation No. R (95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services; Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States on a Guide to human rights for Internet users; Recommendation CM/Rec(2016)1 on protecting and promoting the right to

freedom of expression and the right to private life with regard to network neutrality; and, Recommendation CM/Rec(2016)5 on Internet Freedom.

10. 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;

11. 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;

12. Mindful of the positive obligation on member States to take the measures needed to protect the fundamental rights of everyone within their jurisdiction against serious crimes including acts of terrorism, especially the right to life;

13. 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;

14. Aware that in the fight against serious crimes including acts of terrorism, member States may never act in breach of peremptory norms of international law nor in breach of international humanitarian law;

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

16. Recognising that the use of special investigation techniques is a vital tool for preventing, suppressing and prosecuting the commission of the most serious crimes, including acts of terrorism;

17. 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;

18. 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;

19. 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,

20. 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;

iii. further strengthen international and domestic cooperation in criminal matters to enhance the exchange of information and best practices at the operational level.

Appendix to Recommendation

Chapter I – Definitions and scope

1. 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 preventing, detecting, investigating, prosecuting and suppressing serious crimes, aiming at gathering information in such a way as not to alert the target persons.

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

3. For the purpose of this Recommendation, "financial investigation" means an inquiry into the financial affairs related to a criminal activity, with a view to identifying the extent of criminal networks and/or the scale of criminality; identifying and tracing the proceeds of crime, terrorist funds or any other assets that are, or may become, subject to confiscation; and, developing evidence which can be used in criminal proceedings. This Recommendation also applies when special investigation techniques are used within or for the purpose of financial investigations.

4. For the purpose of this Recommendation, "cyber investigation" means an inquiry aimed at preventing, detecting, investigating, prosecuting and suppressing any serious crimes including acts of terrorism, as well as any criminal offence established by the Council of Europe Convention on the Prevention of Terrorism (CETS No. 196) and its Additional Protocol (CETS No. 217) committed through the Internet and any unlawful interference with information, computer systems, computer programs, and data, that is committed intentionally for the purpose of any serious crimes including acts of terrorism in the context of criminal investigations. This Recommendation also applies when special investigation techniques are used within or for the purpose of cyber investigations.

Chapter II – Use of special investigation techniques at national level

a. General principles

5. Member States should, in accordance with the requirements of the European Convention on Human Rights (ETS No. 5) and the relevant case-law of the European Court of Human Rights, ensure that the circumstances in which, and the conditions under which, the competent authorities are empowered to resort to the use of special investigation techniques are provided for by law with sufficient clarity.

6. Member States should take appropriate legislative measures to allow, in accordance with paragraph 5, 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 for efficient criminal investigation and prosecution. Domestic legislation should afford adequate and effective guarantees against arbitrary and abusive practices, in particular

with regards to the right to a fair trial, the right to respect for private and family life, including the right to protection of personal data, freedom of expression and communication, the right to an effective remedy, and protection of the right of property as enshrined respectively in Articles 6, 8, 10 and 13 of the Convention and Article 1 of Protocol 1 to the Convention.

7. Member States should take appropriate legislative measures to ensure adequate periodical review of the implementation of special investigation techniques by judicial authorities through prior authorisation, supervision during the investigation or ex post facto review.

8. Member States should ensure that an individual or legal person who claims to be the victim of a breach of his rights occasioned by the misuse of special investigation techniques shall have the right of access to an effective remedy before a competent authority.

b. Conditions of use

9. 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.

10. Member States should ensure proportionality between the special investigation techniques used and the legitimate aims pursued. In this respect, when deciding on their use, an evaluation in the light of the seriousness of the offence, the intrusive nature of the specific special investigation technique used, should be made. Also the urgency and general complexity of the case could be considered.

11. Member States should ensure that competent authorities apply less intrusive investigation methods than special investigation techniques if such methods enable the offence to be prevented, detected, investigated, prosecuted and supressed with adequate effectiveness.

12. Member States should take appropriate legislative measures to permit the production of evidence gained from the lawful 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

13. 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.

14. 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 evaluate the opportunity to 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.

15. Member States should make appropriate and expeditious use of special investigation techniques within financial investigations with a view to disrupting the activities of criminal and terrorist associations or groups; identifying and confiscating proceeds and instrumentalities of

serious crimes including acts of terrorism as well as any criminal offence established by the Council of Europe Convention on the Prevention of Terrorism (CETS No. 196) and its Additional Protocol (CETS No. 217).

16. Member States should facilitate the appropriate use of special investigation techniques within financial investigations when enquiries are being made by the competent authorities in all major proceeds-generating offences, money laundering and terrorist financing cases, and in the expeditious identification, tracing, freezing and seizing of property that is or may be subject to confiscation or is suspected of being proceeds of crime.

17. Member States should facilitate the appropriate use of special investigation techniques within cyber investigations in order to prevent, detect, investigate, prosecute and supress the perpetration of cyber-attacks for serious crimes including acts of terrorism, as well as those criminalised under the Council of Europe Convention on the Prevention of Terrorism (CETS No. 196) and its Additional Protocol (CETS No. 217).

18. For the purpose of this Recommendation, member States should ensure, to an appropriate extent, retention and preservation of traffic data by service providers. Such actions should be in accordance with national legislation and applicable international instruments, especially Articles 8 and 10 of 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).

19. 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

20. Member States should ensure adequate training of competent authorities in charge of deciding to use, supervising and using special investigation techniques, including within financial and cyber investigations. 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.

21. 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 – National and international cooperation

22. Member States should make use to the greatest extent possible of existing arrangements for judicial or law enforcement cooperation in relation to the use of special investigation techniques, including within financial and cyber investigations at both a national and international level. Where appropriate member States should also identify and develop additional arrangements, including with the private sector, to enhance cooperation on the fight against serious crimes including acts of terrorism, paying particular attention to questions concerning jurisdiction in connection with the application of special investigation techniques on the internet.

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

Relevant instruments may include, *inter alia*:

- the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances of 20 December 1988;
- the United Nations Convention for the Suppression of the Financing of Terrorism of 9 December 1999;
- 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;
- the Convention on the Prevention of Terrorism of 16 May 2005 (CETS No. 196) and its Additional Protocol of 22 October 2015 (CETS No. 217);
- the Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime of 8 November 1990 (ETS No. 141);
- the Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism of 16 May 2005 (CETS No. 198);
- 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) and its Additional Protocol concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189).

24. Member States are encouraged to make better use, as appropriate, of existing relevant international bodies, such as the United Nations, the Council of Europe, the European Union, the Organization for Security and Co-operation in Europe, the Commonwealth of Independent States, the Global Counterterrorism Forum, INTERPOL and international criminal courts and tribunals, with a view to exchanging experience, further improving international cooperation and conducting best practice analysis in the use of special investigation techniques.

25. 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, also spontaneously, with a view to facilitating the use of special investigation techniques in an international context. If needed, new networks should be developed.

26. 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.

27. 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.