United Nations CTOC/COP/WG.3/2020/3

# Conference of the Parties to the United Nations Convention against Transnational Organized Crime

Distr.: General
12 May 2020

Original: English

**Working Group on International Cooperation**
Vienna, 7 and 8 July 2020
Item 3 of the provisional agenda*
**International cooperation involving special investigative techniques**

## International cooperation involving special investigative techniques

### Background paper prepared by the Secretariat

## I. Introduction

1. In recent years there has been a significant shift in the use of methods to detect and investigate crime and in the nature of investigations, with greater emphasis on intelligence-driven, proactive investigations. In addition, the technological means for gathering information covertly have also advanced rapidly and often involve the use of special investigative techniques. As criminals have become more sophisticated, the methods of detecting and investigating crime also need to evolve and adapt in order to keep pace.

2. Special investigative techniques differ from routine investigation methods and include both covert techniques and the use of technology. They are particularly useful in dealing with sophisticated organized criminal groups, in view of the dangers and difficulties inherent in gaining access to criminal operations and gathering information and evidence for use in domestic prosecutions and criminal proceedings.

3. The need to investigate crime, including transnational organized crime, should be balanced against the respect for the rights and freedoms of individuals when using special investigative techniques. In most jurisdictions, the collection of evidence through such techniques requires strict adherence to a number of safeguards against potential abuses of authority. Moreover, the expanded use of special investigative techniques has to be carefully assessed to ensure that the evidence collected through their means during the investigations meets the applicable evidentiary requirements in subsequent criminal proceedings.

4. The present background paper was prepared by the Secretariat to facilitate discussions under item 3 of the provisional agenda of the eleventh meeting of the Working Group on International Cooperation. It focuses on article 20 of the United Nations Convention against Transnational Organized Crime, while also taking into account developments in the international legal framework and jurisprudence, with the objective of supporting further discussions within the Working Group on the

* CTOC/COP/WG.3/2020/1.

various legal and practical aspects of implementation of article 20, as well as practical ways and means to promote international cooperation involving special investigative techniques, including safeguard measures used in such international cooperation. During those discussions, the Working Group may wish to consider, inter alia, the following issues:

(a) What are the lessons learned from the use of special investigative techniques in the investigation of transnational organized crime?

(b) What are the good practices related to the management of special investigative techniques in the context of transnational organized crime investigations that do not compromise the rights and freedoms of suspects and third parties?

(c) What are the challenges in the implementation of proactive investigation methods when applied to transnational organized crime cases?

(d) What are the most effective and commonly used safeguards against the abuse of special investigative techniques in the context of transnational organized crime cases?

(e) What are the good practices in ensuring the admissibility of evidence in transnational organized crime cases collected through the use of special investigative techniques in other jurisdictions?

# II. Definitional aspects

5. There is no internationally agreed definition of what constitutes “special investigative techniques”. The Organized Crime Convention, the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances of 1988 and the United Nations Convention against Corruption do not provide a definition. There have been attempts to delineate the – equivalent – concept of “special investigative means”, which are perceived as the means or techniques used to gather evidence, intelligence and information in a covert way so as not to alert those being investigated.[1]

6. It should be noted that, in its recommendation Rec(2005)10 to member States on “special investigation techniques” in relation to serious crimes including acts of terrorism, adopted on 20 April 2005, the Committee of Ministers of the Council of Europe has defined “special investigation techniques” as 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.

7. In addition, the specific term “controlled delivery” is defined in article 2, paragraph (i), of the Organized Crime Convention as the “technique of allowing illicit or suspect consignments to pass out of, through or into the territory of one or more States, with the knowledge and under the supervision of their competent authorities, with a view to the investigation of an offence and the identification of persons involved in the commission of the offence”.

# III. Types of special investigative techniques

8. The Organized Crime Convention refers to the appropriate use of controlled delivery (see sect. IV.D below) and provides, where deemed appropriate by the competent authorities of a State party, for the appropriate use of other special investigative techniques, as described below.

[1] See Council of Europe, *The Deployment of Special Investigative Means* (Belgrade, 2013), p. 12.

## A. Electronic surveillance

9. Electronic surveillance includes audio, visual, tracking and data surveillance.[2] The use of electronic evidence-gathering techniques is usually regulated by legislation and, in most countries, through the use of a warrant-based system, especially in cases of electronic surveillance in private places.[3]

10. National laws define in differing terms the circumstances and conditions for issuing a warrant for the use of electronic surveillance. It is generally required that there be reasonable grounds to believe that a relevant offence has been, is being or will be committed. Other factors for consideration include the seriousness of the offence under investigation, the value of the evidence that the surveillance is likely to obtain, whether there are alternative means of obtaining the evidence sought and whether it is in the best interests of the administration of justice to issue the warrant.[4]

11. Regulatory frameworks often contain special provisions for urgent or emergency circumstances requiring the immediate use of electronic evidence gathering or the interception of communications. What constitutes an emergency is usually a serious and imminent threat to national security, persons or property, but may also include circumstances where valuable evidence might be lost without the use of surveillance.[5]

## B. Other forms of surveillance

12. Other forms of surveillance include, on the one hand, physical surveillance and observation, which are generally less intrusive than electronic surveillance and involve placing a target under physical surveillance. On the other hand, they may also extend to monitoring bank accounts in financial investigations.

## C. Undercover and “sting” operations

13. The use of undercover agents, who may or may not be part of an overarching “sting” operation, is valuable in cases where it is very difficult to gain access by conventional means to the activities of criminals or organized criminal groups and therefore necessary to infiltrate criminal networks or pose as offenders to uncover criminal activities.

14. The evidence provided by an “insider”, whether an undercover police officer or even a co-conspirator, can be critical to a successful prosecution. Furthermore, the effect of such conclusive evidence often brings offers of cooperation and pleas of guilt from defendants, thereby eliminating the need for lengthy and expensive trial processes (see also art. 26 of the Organized Crime Convention). Problems may emerge, however, in relation to the legality of the use of undercover officers and sting operations or the admissibility of evidence collected through such means (see sect. VI.B below), in particular because of concerns about entrapment and potential human rights abuses, as well as resources, longevity and the cost of such operations.

## D. Other special investigative techniques

15. The examples of “other special investigative techniques” given in article 20, paragraph 1, of the Organized Crime Convention are not exhaustive, and other

[2] *Current Practices in Electronic Surveillance in the Investigation of Serious and Organized Crime* (United Nations publication, Sales No. E.09.XI.19), p. 2.

[3] Sheelagh Brady, “Policing TOC: the national perspective – challenges, strategies, tactics” in *International Law and Transnational Organized Crime*, Pierre Hauck and Sven Peterke, eds. (Oxford, Oxford University Press, 2016), p. 482.

[4] *Current Practices in Electronic Surveillance*, p. 19.

[5] Ibid., p. 26.

techniques that could be used, where deemed appropriate, include the ones described below.

### 1. Use of informants

16. The use of informants by the police is an important element in the investigation and prevention of crimes. Their role is different from that of witnesses, as they are not called to testify in court and, in some countries, it is not necessary to disclose the assistance that they provide.[6]

17. An informant is a person who establishes or maintains a personal or other relationship with another person for the purpose of facilitating action that covertly uses such a relationship to obtain information or evidence or to provide access to any information or evidence to a third person; or covertly discloses information or evidence obtained by the use of such a relationship, or as a consequence of the existence of such a relationship.[7]

18. Understanding the difference between confidential and non-confidential information and handling accordingly the disclosure of the identity of informants are essential, especially where the informant is closely linked to the criminal activity. In any case, advice from a senior officer, prosecutor or the judiciary should be sought with regard to the use of informants, to ensure the admissibility of the evidence collected. The transnational nature of many organized crime cases requires that investigators be familiar with their own legislation as well as the legislation of the countries with which they cooperate.

### 2. Techniques associated with financial investigations

19. The use of financial institutions for the identification of suspicious financial transactions and their reports to financial intelligence units provide investigators with information about the movement of illicit funds and their connection with suspects. In this context, the use of special investigative techniques (wiretapping, search warrants, witness interviews, search and seizure orders, production orders and account monitoring orders) relates to the examination of financial records or access to documents held by investigators with experience in “following the money trail”, gathering business and financial intelligence, identifying complex illegal schemes and acting quickly to avoid dissipation of the assets.[8]

### 3. Techniques to gather electronic evidence

20. The examination of the legal basis for investigative powers used to gather electronic evidence reveals considerable diversity in national approaches. Nonetheless, a common understanding appears to exist on the types of investigative measures that should be available for gathering electronic evidence. Such measures may include the expedited preservation of computer data; orders for access to stored content data, stored traffic data or subscriber information; the real-time collection of content or traffic data; search warrants for computer hardware or data; the seizure of computer hardware or data; transborder access to a computer system or data; and the use of remote forensic tools.[9]

21. As electronic evidence is, by its very nature, fragile, special precautions should be taken to document, collect, preserve and examine it. The volatile nature of electronic evidence also poses challenges to international cooperation, such as delays in responding to requests, a lack of commitment and flexibility from the authority

[6] United Nations Office on Drugs and Crime (UNODC), *Good Practices for the Protection of Witnesses in Criminal Proceedings Involving Organized Crime* (Vienna, 2008), p. 22.

[7] Council of Europe, *The Deployment of Special Investigative Means*, p. 43.

[8] Jean-Pierre Brun and others, *Asset Recovery Handbook: A Guide for Practitioners* (Washington, D.C., World Bank, 2011), p. 23.

[9] See UNODC, *Comprehensive Study on Cybercrime (Draft)* (February 2013), p. 125, prepared by UNODC for consideration by the Expert Group to Conduct a Comprehensive Study on Cybercrime, and E/CN.15/2018/6, para. 29.

from which evidence is requested and the form in which evidence is provided to the requesting jurisdiction.

22. While many countries have begun to put in place specialized structures for the investigation of crimes involving electronic evidence, such structures remain underfunded in some States and suffer from a lack of capacity. As electronic evidence becomes increasingly pervasive in the investigation of "conventional" crime, law enforcement authorities may need to acquire and deploy basic skills to handle it (CTOC/COP/WG.3/2015/2, para. 12).

# IV. Normative framework: article 20 of the Organized Crime Convention

## A. Article 20, paragraph 1: controlled delivery and other special investigative techniques in domestic legal frameworks

23. Under article 20, paragraph 1, of the Organized Crime Convention, States parties are required, if permitted by the basic principles of their national legal systems, to allow for the appropriate use of controlled delivery, and where appropriate, for the use of other special investigative techniques, such as electronic surveillance and undercover operations in their territory, for the purpose of effectively combating organized crime.

### 1. Constituent elements of the provision

#### (a) "If permitted by the basic principles of [the] domestic legal system"

24. Although paragraph 1 is worded in mandatory terms, the obligation is subject to the basic principles of the domestic legal system of a State party. Hence, the use of investigative techniques should have a proper basis in national legislation, that is, publicly accessible law or laws with an authorization regime that is judicial (or, at least, incorporates judicial oversight). The interference with certain human rights, such as the right to a fair trial[10] and the right to privacy[11] (see below), should be taken into account.

25. According to the jurisprudence of the European Court of Human Rights regarding article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms, the expression "in accordance with the law" also refers to the quality of the law in question. This means that the measure in question should be compatible with the rule of law, publicly accessible for the sake of public scrutiny and foreseeable as to its effects.[12]

26. The requirement of foreseeability means that a rule is formulated with sufficient precision to enable individuals to regulate their conduct. In addition, it implies that there must be a measure of legal protection in domestic law against arbitrary interferences by public authorities. The term "arbitrary" is a key concept in article 17 of the International Covenant on Civil and Political Rights ("No one shall be subjected to arbitrary or unlawful interference with his privacy ..."), which is the legal framework under which the Human Rights Committee, in its capacity as custodian of

[10] Universal Declaration of Human Rights, art. 10, International Covenant on Civil and Political Rights, art. 14, American Convention on Human Rights, art. 8, African Charter on Human and Peoples' Rights, art. 7, and European Convention for the Protection of Human Rights and Fundamental Freedoms, art. 6.

[11] Universal Declaration of Human Rights, art. 12, International Covenant on Civil and Political Rights, art. 17, American Convention on Human Rights, art. 11, and European Convention for the Protection of Human Rights and Fundamental Freedoms, art. 6.

[12] See European Commission of Human Rights, *Malone v. United Kingdom*, application No. 8691/79, judgment of 2 August 1984, paras. 66–67; *Leander v. Sweden*, application No. 9248/81, judgment of 26 March 1987, paras. 50–51; and *Kopp v. Switzerland*, application No. 23224/94, judgment of 25 March 1998, paras. 63–64.

the Covenant, discusses questions relating to the legality and propriety of surveillance measures under its mechanism for review of legislation *in abstracto*.[13] The European Court of Human Rights has also noted in various cases that the law should be sufficiently clear in its terms to give individuals an adequate indication as to the circumstances and conditions under which public authorities are empowered to resort to covert methods.[14]

27. The Court, through its case law on secret measures of surveillance, has developed a set of minimum safeguards that should be statutorily introduced to avoid abuses of power in relation to the following: the nature of the offences that may give rise to a surveillance order; the categories of people liable to be subject to any such measure; a limit on the duration of surveillance; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or destroyed. In addition, the body issuing authorizations should be independent,[15] and there should be either a form of judicial control or control by an independent body over the issuing body's activity.[16] The interception of communications ordered only by the public prosecution without any prior control possibility by a judge does not meet the required standards of independence.[17]

### (b) "Under the conditions prescribed by … domestic law"

28. By referring to the "conditions prescribed by … domestic law", the Organized Crime Convention calls upon States parties to define in their national legislation the circumstances and conditions under which the competent authorities are empowered to use special investigative techniques.

29. Most special investigative techniques are highly intrusive and may give rise to constitutional difficulties as regards their compatibility with fundamental rights and freedoms. States parties may therefore decide not to allow certain techniques under their domestic legal systems. In addition, the reference to conditions prescribed by domestic law enables States parties to subject the use of these special investigative techniques to as many safeguards and guarantees as may be required for the protection of human rights and fundamental freedoms.

30. In its jurisprudence regarding the interception of communications, the European Court of Human Rights has established that the following minimum safeguards should be prescribed in a statute regulating a covert activity: a definition of the categories of people liable to have their telephones tapped by judicial order; the nature of the offences that may give rise to such an order; a limit on the duration of telephone tapping; a procedure for drawing up summary reports containing intercepted communications; the precautions to be taken to communicate the recordings intact

---

[13] The term "arbitrariness" has been redefined by the Human Rights Committee in its general comment No. 35 (2014) on article 9 (Liberty and security of person), albeit in the different context of "arbitrary detention", in the following manner: "The notion of 'arbitrariness' is not to be equated with 'against the law', but must be interpreted more broadly to include elements of inappropriateness, injustice, lack of predictability and due process of law, as well as elements of reasonableness, necessity and proportionality" (CCPR/C/GC/35, para. 12). Applying this legal standard when reviewing the "arbitrariness" of online surveillance, would appear to invite an evaluation of the predictability of the application of surveillance powers, the fairness of the procedure governing their application, the potential for their excessive use and the availability of safeguards against abuse.

[14] European Commission of Human Rights, *Kopp v. Switzerland*, para. 64; *Khan v. United Kingdom*, application No. 35394/97, judgment of 12 May 2000, para. 26; and *Taylor-Sabori v. United Kingdom*, application No. 47114/99, judgment of 22 October 2002, para. 18.

[15] *Malone v. United Kingdom*, para. 67.

[16] European Commission of Human Rights, *Huvig v. France*, application No. 11105/84, judgment of 24 April 1990, para. 33; *Amann v. Switzerland*, application No. 27798/95, judgment of 16 February 2000, para. 60; and *Iordachi and others v. Moldova*, application No. 25198/02, judgment of 10 February 2009, para. 40.

[17] European Commission of Human Rights, *Dumitru Popescu v. Romania* (No. 2), application No. 71525/01, judgment of 26 April 2007, paras. 70–73.

and in their entirety for possible inspection by the judge and the defence; and the circumstances in which recordings may or must be erased or tapes destroyed, in particular where an accused has been discharged by a magistrate or acquitted by a court.

### (c) "Necessary measures"

31. What is "necessary" and when the use of special investigative techniques is "appropriate" (see below) are a matter of judgment. In accordance with settled case law of the European Court of Human Rights, an interference with human rights will be considered necessary for a legitimate aim if it responds to a so-called "pressing social need", in particular if it is proportionate to the legitimate aim pursued and if the reasons adduced by the national authorities to justify it are "relevant and sufficient".

32. In relation to secret surveillance, the Court has held that national authorities enjoy a fairly wide margin of appreciation in choosing the means for achieving the legitimate aim of protecting national security.[18] The breadth of this margin varies, depending on a number of factors, including the nature of the Convention right at stake in a given case, its importance for the individual, the nature of the interference and the object pursued by the interference.

### (d) "Within [the State party's] possibilities"

33. This clause takes into account the limited technical capacities and resources in many States parties to undertake an operation involving a particular investigative technique. The clause is reinforced by an interpretative note to paragraph 1 of article 20, in which it is indicated that that paragraph "does not imply an obligation on States parties to make provisions for the use of all the forms of special investigative technique noted".[19]

### (e) "Appropriate use"

34. The "appropriate use" of special investigative techniques is tightly linked to the proportionality between the effects of their use and their objective. Such proportionality should be tested and ensured before the techniques are resorted to. In this regard, when deciding on the use of such techniques, the competent authorities should make an assessment in the light of the seriousness of the offence in question and assess whether the intrusive nature of the specific special investigative technique is justified.

35. Factors to consider in determining whether a covert measure is proportionate to the aim pursued include the seriousness of the offence vis-à-vis the intrusive nature of the specific special investigative techniques used,[20] whether relevant and sufficient reasons have been advanced in support of the measure, whether a less restrictive alternative measure was available, whether there has been some measure of procedural fairness in the decision-making process, whether adequate safeguards against abuse exist and whether the restriction under scrutiny destroys the very essence of the right in question.[21]

---

[18] *Malone v. United Kingdom*, para. 81, and *Leander v. Sweden*, para. 59.

[19] See the *Travaux Préparatoires of the Negotiations for the Elaboration of the United Nations Convention against Transnational Organized Crime and the Protocols thereto* (United Nations publication, Sales No. E.06.V.5), p. 206. See also David McClean, *Transnational Organized Crime: A Commentary on the UN Convention and its Protocols*, Oxford Commentaries on International Law Series (Oxford, Oxford University Press, 2007), p. 244.

[20] Recommendation Rec(2005)10 of the Council of Europe Committee of Ministers to member States on "special investigation techniques" in relation to serious crimes including acts of terrorism, appendix, chap. II, para. 5.

[21] See Council of Europe, *The Deployment of Special Investigative Means*, p. 17.

### (f) "By [the] competent authorities"

36. For the purpose of recommendation Rec(2005)10 of the Council of Europe Committee of Ministers to member States on "special investigation techniques" in relation to serious crimes including acts of terrorism, "competent authorities" means judicial, prosecuting and investigating authorities involved in deciding, supervising or using special investigation techniques in accordance with national legislation.[22]

37. The competence of authorities involved in controlled deliveries, in particular, is linked to the question of whether or not a request for mutual legal assistance is a precondition for authorizing a controlled delivery. Such a request is required mainly in jurisdictions in continental Europe. In some jurisdictions, it is an obligatory precondition only when the controlled delivery is requested in the context of an ongoing criminal investigation or criminal case. Requests for mutual assistance are not needed when the controlled delivery is linked to an operational investigatory file. On the other hand, in most common law jurisdictions, a request for mutual legal assistance is not a sine qua non requirement for the authorization of controlled deliveries. In those jurisdictions, the authorities will be content with requests made on a police-to-police basis.

### (g) "In the territory [of a State party]"

38. Paragraph 1 of article 20 focuses on domestic aspects of special investigative techniques and refers to relevant action to be taken within the territory of each State party to the Convention. The international aspects, that is, the international cooperation needed for using such techniques, are addressed in paragraphs 2 and 3.

## 2. Implementation and enforcement

39. The issue of joint investigations and the related review of the implementation of article 20 of the Convention will be examined under the cluster on law enforcement and the judicial system of the newly established Mechanism for the Review of the Implementation of the United Nations Convention against Translational Organized Crime and the Protocols thereto (years VII–X of the multi-year workplan for the functioning of the Mechanism).[23] The Mechanism will function on the basis of procedures and rules adopted by the Conference of the Parties to the United Nations Convention against Transnational Organized Crime at its ninth session, in October 2018, in its resolution 9/1.

40. For comparative purposes, in the first cycle of the Mechanism for the Review of the Implementation of the United Nations Convention against Corruption, the majority of States parties under review reported that they regulated the scope of special investigative techniques, as well as the conditions and procedures for using them, through legislation or established practice. Overall, most countries were familiar with, and resorted to, special investigative techniques, even though those were commonly used within the context of investigations related to organized crime, drug trafficking and, to a lesser extent, corruption. An impediment identified at the operational level was the lack of capacity and experience in many countries with the use of these techniques. A general trend in many jurisdictions was to resort to such techniques in relation to more serious crimes, as defined under national law.[24]

[22] See recommendation Rec(2005)10, appendix, chap. I.

[23] See CTOC/COP/2018/13, resolution 9/1, appendix, table 2.

[24] See the relevant analysis of findings emerging from country reviews in *State of Implementation of the United Nations Convention against Corruption: Criminalization, Law Enforcement and International Cooperation*, 2nd ed. (Vienna, 2017), p. 255.

## B. Article 20, paragraph 2: bilateral and multilateral agreements or arrangements (the international cooperation aspect)

41. Paragraph 2 of article 20 accords priority to international agreements on the use of special investigative techniques and therefore encourages States parties to conclude bilateral or multilateral agreements or arrangements to foster cooperation in this field, with due respect to national sovereignty concerns.

42. At the international level, the 1988 Convention was the first multilateral agreement to endorse the investigative technique and practice of controlled delivery (art. 11).[25] Article 50 of the Convention against Corruption regulates issues pertaining to special investigative techniques, building on the precedent of article 20 of the Organized Crime Convention.

43. At the regional level, a number of special investigative techniques were included in the Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders (arts. 39–41 and 73).[26] Other examples of regional conventions providing for special investigative techniques include the Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (art. 4),[27] the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union (arts. 12, 14 and 17–20),[28] the Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters (arts. 17–19)[29] and, to the extent applicable, the Council of Europe Convention on Cybercrime.[30]

44. Within the context of the European Union, a new instrument developed to facilitate cross-border investigation is Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters. The Directive includes provisions on covert investigations (art. 29) and the interception of telecommunications (arts. 30–32).

45. The term “arrangements” denotes the most informal type of interaction and may include standard practices mutually applied by the competent authorities of each State party in related situations, including cooperation among police officials without the need for formal written agreements.

46. Recommendation 31 of the Financial Action Task Force Recommendations addresses the powers of law enforcement and investigative authorities and specifies that countries should ensure that competent authorities conducting investigations are

[25] *Commentary on the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances 1988* (United Nations publication, Sales No. E.98.XI.5), article 11, general comments, para. 11.2.

[26] See Hans G. Nilsson, “Special investigation techniques and developments in mutual legal assistance: the crossroads between police cooperation and judicial cooperation”, in *Resource Material Series No. 65* (Tokyo, Asia and Far East Institute for the Prevention of Crime and the Treatment of Offenders, 2005), pp. 42–43.

[27] United Nations, *Treaty Series*, vol. 1862, No. 31704. The Convention entered into force on 1 September 1993. For further analysis on the nature of those measures, see the Explanatory Report to the Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime, para. 30.

[28] *Official Journal of the European Communities*, C 197/1, 12 July 2000. See also the Explanatory Report on the Convention of 29 May 2000 on Mutual Assistance in Criminal Matters between the Member States of the European Union (*Official Journal of the European Communities*, C 379/7, December 2000).

[29] United Nations, *Treaty Series*, vol. 2297, No. 6841. The Protocol entered into force on 1 February 2004.

[30] Council of Europe, *European Treaty Series*, No.185. The Convention entered into force on 1 July 2004.

able to use a wide range of investigative techniques suitable for the investigation of money-laundering, associated predicate offences and terrorist financing.[31]

47. At the implementation and enforcement levels, international cooperation can be supported through specific agreements or arrangements or through mutual legal assistance agreements. Non-coercive investigative techniques can often be used through informal assistance, while coercive investigative techniques and judicial measures typically require a request for mutual legal assistance.[32] Furthermore, informal and formal networks of those involved in the investigation of crimes are increasingly valuable for the smooth operation of cross-border cooperation.

## C. Article 20, paragraph 3: use of special investigative techniques on a case-by-case basis

48. Paragraph 3 of article 20 refers to the practice of using special investigative techniques at the international level in the absence of agreements or arrangements. The provision calls upon States parties to cooperate on a case-by-case basis. For a number of States, this provision will itself be a sufficient source of legal authority for case-by-case cooperation.

49. In addition to the obvious operational arrangements, two particular factors are identified in paragraph 3 as potentially needing attention. The first one relates to financial arrangements, which include the cost of using those techniques, bearing in mind not only the resources that need to be deployed but also the needs of each State party (for example, for taking evidence in a particular form). Although there is a link, in some cases, between the use of special investigative techniques at the international level and mutual legal assistance, the costs of such use are not generally treated as "ordinary costs" for the purposes of article 18, paragraph 28, of the Convention.[33] The complexity of these issues makes it desirable to have in place standing arrangements or memorandums of understanding, as there may be no time for detailed negotiations in certain cases.

50. The second factor relates to the exercise of jurisdiction in cases where the evidence collected through special investigative techniques show that the criminal offences are linked to other States as well. For purposes of clarity, this possibility may be taken into account by the competent authorities, if time permits, before any conflicting claims to jurisdiction arise. In any case, consultations may be needed among the States parties concerned to coordinate their actions and resolve jurisdiction conflicts, in line with article 15, paragraph 5, of the Organized Crime Convention.

51. For comparative purposes, in the context of the Mechanism for the Review of the Implementation of the Convention against Corruption, the reported data demonstrated that special investigative techniques can be used at the international level even in the absence of relevant international agreements and on a case-by-case basis in a large number of States parties to the Convention. Some of those States have authorized such techniques only on the condition of reciprocity.

## D. Article 20, paragraph 4: controlled delivery and related methods

52. Paragraph 4 of article 20 clarifies that the methods of controlled delivery that may be applied at the international level include intercepting and allowing goods to continue intact, intercepting and removing them and intercepting and replacing them

[31] See Financial Action Task Force, *International Standards on Combating Money-Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations* (Paris, June 2019).

[32] Brun and others, *Asset Recovery Handbook*, p. 131.

[33] See, for comparative purposes, the *Commentary on the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances 1988*, article 11, paragraph 2, para. 11.18.

in whole or in part. The provision leaves the choice of method to the State party concerned.

53. Controlled delivery is an investigative tool that is not a distinct special investigative technique in itself, even though it is often described as such. Rather, it is a technique that, typically, uses a range of special investigative means, usually surveillance, undercover deployment and interception (both of the item and of communications).

54. Controlled delivery is useful in cases where contraband is identified or intercepted in transit and then delivered under surveillance to identify the intended recipients or to monitor its subsequent distribution throughout a criminal organization. Moreover, the controlled delivery of funds known or suspected to be the proceeds of crime is a valid and effective law enforcement technique for obtaining information and evidence, in particular in the context of international money-laundering operations.

55. In smuggling of migrants cases, controlled deliveries can also be used by allowing an organized criminal group to move migrants in order to discover the identity of offenders or identify the premises used. Controlled deliveries are often conducted through joint investigations because of the cross-border nature of the offences, where cooperation among immigration and law enforcement authorities is essential and where appropriate authorization must be obtained (CTOC/COP/WG.7/2013/2, para. 27).

56. Legislative provisions are often required to permit such a course of action, as the delivery of the contraband by a law enforcement agent or other person may itself be a crime under domestic law.[34] For evidence acquired in the course of controlled operations to be used in judicial proceedings, many States require specific legal authority for such operations in their own domestic legal frameworks, and sometimes in those of other States participating in the controlled delivery.

57. Detailed advanced planning is necessary to ensure the smooth and effective administration and control of duly approved operations. In this regard, procedures for domestic inter-agency cooperation are vital. Practice has demonstrated the utility for many countries of designating a centralized authority to facilitate coordination and prevent confusion, confrontation and risk. In jurisdictions where such an option would not be appropriate, the creation of an internal, and possibly institutionalized, coordination mechanism may be considered.

# V. Soft law

58. The *Model Legislative Provisions against Organized Crime*, developed by the United Nations Office on Drugs and Crime to promote and assist the efforts of Member States to become parties to and implement the provisions of the Organized Crime Convention and the Protocols thereto, provide further guidance on the development of legislation in this field. Chapter IV of the Model Legislative Provisions, in particular, provides, inter alia, a basic legal framework to support the use of special investigative techniques that may assist in effectively responding to complex transnational crimes. Article 13 of that chapter focuses on controlled deliveries, article 14 on the acquisition and use of assumed identities, article 15 on infiltrations and article 16 on electronic surveillance.

# VI. Human rights considerations

59. Because of their multiple types, special investigative techniques may raise human rights issues at various levels. For example, it may be appropriate for a

[34] UNODC, *Legislative Guide for the Implementation of the United Nations Convention against Transnational Organized Crime* (Vienna, 2016), para. 443.

controlled delivery to be authorized by senior law enforcement officials, whereas electronic surveillance usually requires judicial authorization and supervision. Accordingly, each major type of special investigative techniques should be addressed individually so that an appropriate regime may be established for each.

60. The aforementioned Council of Europe Committee of Ministers recommendation Rec(2005)10 on "special investigation techniques" in relation to serious crimes including acts of terrorism offers a useful reference tool for further consideration. The Committee of Ministers notes therein the need to maintain a balance between ensuring public safety through law enforcement and securing the rights of individuals. It also recognizes that the development of common standards would contribute to public confidence in the use of special investigative techniques. The Committee of Ministers sets out a number of principles to guide States in the formulation of national laws and policies, including the importance of adequate control of implementation of special investigative techniques by judicial authorities or other independent bodies through prior authorization, supervision during the investigation or after the fact review; the importance of ensuring proportionality of the special investigative technique used when compared with the conduct being investigated (following the principle that the least invasive method suitable to achieve the objective should be used); the need for States to enact laws to permit the production of evidence gained through special investigative techniques in court, while respecting the right to a fair trial; the importance of operational guidelines and training in the use of special investigative techniques; and the need for States to make the greatest possible use of existing international arrangements for judicial and police cooperation in relation to the use of specialist investigative techniques, supplemented by additional arrangements, where necessary.

61. It is important that special investigative techniques be subject to a level of scrutiny to avoid their misuse. It is recommended in the *Model Legislative Provisions against Organized Crime* that a senior official be required to report to parliament, or equivalent, on an annual basis, on the number of authorizations sought and granted and the number of prosecutions where evidence or information obtained through authorizations was used. In some legal systems, there may be a preference for additional scrutiny through, for example, reporting and review by an independent oversight body. In that case, it will likely be necessary to have two levels of review: one that allows full review, including access to sensitive operational information, carried out by an independent review body with a specific legislative mandate; and a second, which is a public review for parliament or other, that does not disclose operational information, including methods and sources.[35]

## A. The use of modern means of technology and its impact on human rights

62. Technology-based tools that can be used in investigations as innovative elements of sophisticated special investigative techniques may prove to be useful entry points for addressing crime-related threats. However, caution is needed in the specific application of those tools to ensure responsible and ethical use and avoid unintended consequences. This is particularly important given that many of the present and future technologies could carry serious implications for personal privacy and civil liberties.[36]

63. The proliferation of biometrics and data collection systems can have a corrosive effect on privacy where proper control or oversight is absent or weak. Moreover, facial recognition software is being used by law enforcement professionals to identify suspects much more rapidly. However, critics worry that it may lead to abusive government surveillance, corporate manipulation and the end of privacy.

[35] UNODC, *Model Legislative Provisions against Organized Crime* (Vienna, 2012), p. 64.
[36] A/CONF.234/11, para. 70.

Furthermore, the data retention aspect of biometric systems may jeopardize privacy through potential data misuse.[37]

64. A balanced approach is therefore needed to find solutions where technology and privacy or other human rights seem to be on a collision course. To avoid the use of technologies as a "Trojan horse" for potential infringements of fundamental rights, technology development needs to be continuously monitored and its impact evaluated.[38]

65. In its resolution 68/167 on the right to privacy in a digital age, the General Assembly reaffirmed the human right to privacy, according to which no one shall be subject to arbitrary and unlawful interference with his or her right to privacy. It called upon all States to: review their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law; and establish or maintain existing independent, effective domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data.

## B. Admissibility of evidence and fair trial considerations

66. An important factor in the use of special investigative techniques is the need to comply with procedural safeguards for the admissibility in court of the evidence obtained through such techniques, including those involving the use of modern technology. In most jurisdictions, the process of gathering evidence requires strict adherence to a number of safeguards against potential abuses of authority, including judicial or independent oversight of the use of those techniques and observance of the principles of legality, subsidiarity and proportionality.[39]

67. The admissibility of electronic evidence, in particular, requires compliance with established procedures that safeguard human rights (E/CN.15/2018/6, para. 30). When assessing the admissibility of electronic evidence, emphasis should be placed on the importance of compliance with the proportionality principle when using special investigative techniques in cybercrime investigations, including the use of undercover agents and remote forensics, especially on the darknet (UNODC/CCPCJ/EG.4/2019/2, para. 37).

68. Moreover, the application of general principles of domestic procedural laws and national jurisprudence pertaining to the admissibility of evidence obtained in forensic cryptocurrency investigations is a new challenging area for further consideration and sharing of experiences, owing to the innovative techniques used in that context.[40]

69. Article 20, paragraph 1, of the Organized Crime Convention does not require States parties to take such measures as to allow for the admissibility in court of evidence derived from the use of special investigative techniques as article 50, paragraph 1, of the Convention against Corruption explicitly does. This is an element which refers to the positive obligation of a State party to have in place laws, regulations and procedures to enable, for the sake of legal certainty, proper

[37] See Max Snijder, *Biometrics, Surveillance and Privacy: ERNCIP Thematic Group Applied Biometrics for the Security of Critical Infrastructure* (Luxembourg, Publications Office of the European Union, 2016), p. 4.

[38] A/CONF.234/11, para. 78.

[39] Dimosthenis Chrysikos, "Special investigative techniques", in *The United Nations Convention against Corruption: A Commentary*, Cecily Rose, Michael Kubiciel and Oliver Landwehr, eds., Oxford Commentaries on International Law Series (Oxford, Oxford University Press, 2019), p. 507.

[40] Michael Fröwis and others, "Safeguarding the evidential value of forensic cryptocurrency investigations" (June 2019).

administration of justice and human rights protection, the admissibility before a court of evidence resulting from the use of special investigative techniques.

70. Despite the lack of this element in paragraph 1 of article 20, it is vital for drafters of national legislation to consider the issue of whether evidence obtained through, for example, infiltration or undercover operations can be adduced in court and, if so, whether the undercover agents have to reveal their real identity. It is important to balance the interests of justice (including the need to combat transnational organized crime) with the need to ensure a fair trial of the accused.[41]

71. Both the Organized Crime Convention and the Convention against Corruption are silent on the issue of the legal value of information collected through special investigative techniques. Decisions pertaining to the conditions for using such information as admissible evidence in court are thus left to the discretion of the State concerned, taking into account the basic principles of its legal system and the legalization and authentication methods prescribed by its law.

72. In its jurisprudence, the European Court of Human Rights has repeatedly stated that the admissibility of evidence was primarily a matter for regulation under national law. As a rule, it is for the national courts to assess the evidence before them. The role of the European Court is to examine whether the proceedings as a whole, including the way in which the evidence was obtained, were fair and whether they resulted in an infringement of article 6 of the European Convention on Human Rights.

73. The application of special investigative techniques, in particular undercover operations, cannot in itself constitute an infringement of article 6, paragraph 1, of the European Convention on Human Rights, but their use is subject to restrictions and safeguards. Regarding the limits to the involvement of undercover agents in undercover operations, the European Court of Human Rights makes a clear distinction between an undercover agent and an agent provocateur. The former's activity is confined to gathering information, while the latter actually incites people to commit a criminal act. In the case of *Ramanauskas v. Lithuania*,[42] the Court formulated the concept of entrapment in breach of article 6, paragraph 1, as follows:

> Police incitement occurs where the officers involved – whether members of the security forces or persons acting on their instructions – do not confine themselves to investigating criminal activity in an essentially passive manner, but exert such an influence on the subject as to incite the commission of an offence that would otherwise not have been committed, in order to make it possible to establish the offence, that is, to provide evidence and institute a prosecution.

74. Any covert operation should comply with the requirement that the investigation be conducted in an "essentially passive manner". If it is established by the court that a person was incited to commit a criminal act and the evidence resulting from such activity is the only one on which the finding of a person's guilt is based, there are grounds for recognizing the breach of the right to a fair trial.[43]

75. Factors to be taken into account when assessing whether the acts of the undercover agents went beyond the mere passive investigation of pre-existing criminal activity and amounted to police incitement include: reasonable grounds or good reason to suspect that the person is involved in preliminary acts to commit the relevant criminal conduct, had committed a criminal act beforehand or had the disposition to become involved in the commission of a criminal offence until the approach by the police; (linked to the previous one) the starting point of the

[41] UNODC, *Model Legislative Provisions*, p. 70.

[42] European Court of Human Rights, *Ramanauskas v. Lithuania*, application No. 74420/01, judgment of 5 February 2008.

[43] Ibid., para. 54; *Teixeira de Castro v. Portugal*, application No. 25829/24, judgment of 9 June 1998, paras. 35–36 and 39; *Bannikova v. Russia*, application No. 18757/06, judgment of 4 November 2010, para. 34; and *Baltiņš v. Latvia*, application No. 25282/07, judgment of 8 January 2013, para. 55.

undercover operation; the legality of the undercover agents' activity; and the scope of the undercover agents' involvement (i.e., whether they took the initiative to start the communication with the targeted person, and whether there was pre-existing negotiation or agreement).

76. From a procedural point of view, the protection of the principles of adversarial process and equality of arms should be taken into account, the prosecution bearing the burden of proof to demonstrate that there was no incitement. In addition, under article 6, paragraph 1, of the European Convention on Human Rights, prosecution authorities are required to disclose to the defence all material evidence in their possession for or against the accused.

# VII. Conclusions and recommendations

77. The present paper focuses on the different types of special investigative techniques, in particular those that can be used in the investigation of transnational organized crime, as well as the main constituent and implementation elements of article 20 of the Organized Crime Convention.

78. The Working Group on International Cooperation may wish to consider the various issues and questions raised in the introduction (sect. I) as a basis for its deliberations.

79. The Working Group may also wish to use the present paper as reference material and bring to the attention of the Conference of the Parties the main conclusions of the discussion facilitated by the paper, with a view to highlighting the necessity of further work in this area, subject to the availability of resources. Such work could implement a previous recommendation of the Conference contained in its resolution 5/8 and, thus, take the form of a matrix identifying legal and practical issues that could arise in the implementation of article 20 of the Organized Crime Convention and the use of special investigative techniques, as well as possible solutions to those issues, including by collecting examples of arrangements or agreements on the use of such techniques between States parties; or could take the form of legal, practical and operational guidelines on the implementation of article 20.

80. The Working Group may further wish to recommend that the Conference:

(a) Continue to encourage States parties to make use, where appropriate, of article 20 of the Organized Crime Convention as a legal basis for international cooperation to carry out special investigative techniques;

(b) Encourage States parties to exchange best practices and lessons learned in the field of special investigative techniques, especially those relating to the implementation of article 20 of the Convention; and

(c) Encourage States parties to facilitate training activities for judges, prosecutors, law enforcement officers or other practitioners engaged in the conduct or oversight of special investigative techniques, and invite the Secretariat, subject to the availability of resources, to develop and implement technical assistance activities in this area.