Bulletin of the *Transilvania* University of Braşov
Series VII: Social Sciences • Law • Vol. 16(65) Special Issue – 2023
https://doi.org/10.31926/but.ssl.2023.16.65.3.23

PROCEDURAL ASPECTS OF THE SECOND ADDITIONAL PROTOCOL TO THE COUNCIL OF EUROPE CONVENTION ON CYBERCRIME

Adrian Cristian MOISE[1]

Abstract: *The objective of the second protocol is to strengthen cooperation in cybercrime and the collection of electronic evidence of crimes for the purpose of specific criminal investigations or proceedings. The article also presents and analyzes the most important procedural aspects related to the second additional protocol to the Council of Europe Convention on cybercrime regarding enhanced cooperation and the disclosure of electronic evidence. The analysis of the second additional protocol takes into account the provisions of the Council of Europe Convention on Cybercrime.*

Key words: *cooperation, cybercrime, video conferencing, digital evidence, criminal investigation.*

1. Introduction

Cybercrime continues to pose a considerable challenge to our society. Despite the best efforts of law enforcement and judicial authorities, cyber attacks, including ransomware attacks, are increasing and becoming more sophisticated.

The phenomenon of cybercrime has a global dimension, characterized by multiple territorial links. The cybercriminal is subject to the jurisdiction of a particular country, but his illegal actions may target computer systems and people in many other countries. The development of the Internet has created new opportunities for cybercriminals to commit cybercrimes remotely.

In such a context, international cooperation in the field of combating cybercrime between law enforcement bodies is required to achieve results in investigative processes.

The general objective of the second additional protocol to the Council of Europe Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence is to strengthen cooperation in cybercrime and the collection of electronic evidence of crimes for the purpose of specific criminal investigations or proceedings.

[1] Spiru Haret University of Bucharest, Faculty of Juridical, Economic and Administrative Sciences, Craiova, adriancristian.moise@gmail.com.

The second additional protocol to the Council of Europe Convention on Cybercrime recognizes the need for increased and more effective cooperation between States and with the private sector, as well as greater legal clarity and certainty for service providers and other entities regarding the circumstances in which they can respond to requests from the criminal justice authorities of other parties regarding disclosure of electronic evidence.

The second additional protocol to the Council of Europe Convention on Cybercrime also recognizes that effective cross-border criminal justice cooperation, including between public sector authorities and private sector entities, requires effective conditions and solid safeguards for the protection of fundamental rights.

To this end, the second additional protocol to the Council of Europe Convention on Cybercrime adopted a rights-based approach and provides conditions and guarantees in accordance with international human rights instruments, including the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms.

Chapter I of the second additional protocol to the Council of Europe Convention on Cybercrime stipulates common provisions, in the sense that the purpose of this protocol is to supplement the Convention as between the Parties to this Protocol.

Article 2 sets out the scope of the second additional protocol, in accordance with the scope of the Convention on Cybercrime: it applies to investigations or specific criminal proceedings relating to crimes related to information systems and data, as well as to the collection of evidence in digital format regarding crimes.

Article 3 includes definitions of "central authorities", "competent authorities", "emergency situations", "personal data" and "transferring parties". These definitions apply to the Protocol, together with the definitions included in the Convention on Cybercrime.

Article 4 sets out the languages in which the parties should transmit orders, requests or notifications under the second additional protocol.

Chapter II of the second additional protocol provides for measures to strengthen cooperation. First, Article 5(1) states that the Parties shall cooperate on the basis of the protocol to the greatest extent possible. Article 5 paragraphs (2)-(5) establishes the application of the measures stipulated in the protocol in relation to existing treaties or agreements on mutual assistance.

Article 5 (7) provides that measures in Chapter II do not restrict cooperation between the Parties or with service providers or entities, through other applicable agreements, understandings and practices or applicable domestic law.

Article 6 provides a basis for direct cooperation between the competent authorities of a Party and entities of another Party that provide domain name registration services for the disclosure of domain name registration data.

Article 7 provides a basis for direct cooperation between competent authorities of a Party and service providers of another Party for the disclosure of subscriber data.

Article 8 provides a basis for enhanced cooperation between authorities regarding the disclosure of computer data.

Article 9 provides a basis for cooperation between authorities regarding the disclosure of computer data in emergency situations.

Article 10 provides a basis for mutual legal assistance in emergency situations. Article 11 provides a basis for cooperation through videoconferencing.

2. Procedural aspects of the second additional protocol to the Council of Europe Convention on Cybercrime

Article 5, paragraph 1, makes clear that, as in Article 23 and Article 25, paragraph 1, of the Convention, the Parties shall cooperate, in accordance with the provisions of Chapter II, "to the fullest extent possible". This principle requires parties to provide extensive cooperation and minimize obstacles to the smooth and rapid flow of information and evidence at the international level.

Paragraphs 2-5 of the Article 5 from the second additional protocol organize the seven cooperation measures of this protocol into four different sections following the first section on general principles (Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence. Explanatory Report, 2021, p. 46).

These sections are divided according to the types of cooperation sought: section 2 covers direct cooperation with private entities; section 3 contains forms of consolidated international cooperation between authorities for the disclosure of stored data; section 4 provides for mutual assistance in case of emergency; section 5 concludes with provisions for international cooperation to be applied in the absence of a treaty or agreement based on uniform or reciprocal legislation between the parties concerned.

We have noted that these sections are also roughly organized in a progression from the forms of investigative assistance often sought at the beginning of an investigation, to obtain disclosure of domain name registration and subscriber information, to requests for traffic data and then content data, followed by video-conferencing.

In reviewing these provisions above, we noted that the second additional protocol does not eliminate or restrict any cooperation between Parties or between Parties and private entities that is otherwise available – whether through applicable agreements, arrangements, domestic law or even informal practices.

The drafters of the second additional protocol intended to expand, not narrow, the tools available in the law enforcement practitioner's toolbox to obtain information or evidence for specific criminal investigations or proceedings.

The drafters also recognized that in some situations existing mechanisms such as mutual assistance may be best for a practitioner to use. However, in other situations, the tools created by this second additional protocol may be more effective or preferable.

For example, if a competent authority needs content data in an emergency, it would likely choose to use a traditional request for mutual assistance under a bilateral treaty or under Article 27 of the Convention on Cybercrime, as appropriate, as the second additional protocol does not contain provisions for obtaining content data on a non-emergency basis. But in the event that it needed information about the subscriber, it could choose to use Article 7 of the second additional protocol to issue a command directly to a service provider.

Article 6 establishes a procedure that provides for direct cooperation between the authorities of a Party and an entity providing domain name registration services in the territory of another Party to obtain information about domain name registrations on the Internet.

Nowadays many forms of cybercrime are facilitated by criminals who create and exploit domains for malicious and illicit purposes. For example, a domain name can be used as a platform for spreading malware, botnets, phishing and similar activities, fraud, distribution of child abuse material and other criminal purposes.

We believe that access to information about the legal or natural person who registered a domain is therefore essential to identify a suspect in a particular investigation or criminal procedure, this provision being a very good thing for the field of computer crime investigation.

The Article 6 procedure also recognizes the current model of Internet governance, which is concerned with the development of multiple consensus-based policies. These policies are normally based on contract law and the procedure set out in the Article 6 is intended to supplement these policies in the second additional protocol sense, such as for the purpose of specific criminal investigations or proceedings (Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence. Explanatory Report, 2021, p. 50).

Article 7 establishes a procedure that provides for direct cooperation between the authorities of a Party and a service provider in the territory of another Party to obtain information about the subscriber (Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence. Explanatory Report, 2021, p. 53-54).

Subscriber information is the information most often sought in criminal investigations of cybercrime and other types of crimes that require electronic evidence. An increasing number of criminal investigations or proceedings now require access to digital evidence from service providers in other countries. Even for types of crimes where the offender, victim and perpetrator are all in the same country as the investigating authority, digital evidence may be held by a service provider in another country.

We believe that the law enforcement bodies investigating a crime may be required to use international cooperation procedures, such as mutual assistance, which are not always able to provide assistance quickly or efficiently enough for the needs of the criminal investigations or proceedings due to the increase in the volume of requests for digital evidence.

Although the Article 18 of the Council of Europe Convention on Cybercrime already addresses some aspects of the need for rapid and effective access to digital evidence from service providers, it does not in itself provide a complete solution to this challenge, as this Article applies in a more limited set of circumstances, thus the legislators adopted the Article 7 of the second additional protocol.

Article 8 of the second additional protocol provides that a requesting party has the ability to issue an order to be served as part of an application to another party and that the requested party has the ability to enforce that order by compelling a service

provider in its territory to produce subscriber information or traffic data in the service provider's possession or control.

Thus, Article 8 establishes a mechanism that complements the mutual assistance provisions of the Convention, in that the information that the requesting party must provide is more limited and the process of obtaining data is faster (Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence. Explanatory Report, 2021, p. 61-62).

We consider that this article complements and is therefore without prejudice to other processes of mutual assistance under the Council of Europe Convention on Cybercrime or other multilateral or bilateral agreements, which a party remains free to invoke.

Cybercrime investigations usually require an immediate response, especially when traffic data, which is needed to identify a suspect, is disposed of in a short period of time. In order to increase the speed of international investigations, the Council of Europe Convention on Cybercrime emphasized the importance of using fast means of communication in the Article 25.

In order to improve the efficiency of requests for mutual legal assistance, the legislators of the Council of Europe Convention on Cybercrime obliged the parties to designate a contact point for requests for mutual legal assistance, which is available without a time limit. Moreover, the authors of the Council of Europe Convention on Cybercrime emphasized that establishing contact points is one of the most important tools provided by the Council of Europe Convention on Cybercrime.

Article 35 of the Council of Europe Convention on Cybercrime defines the minimum characteristics required for the network contact points.

Apart from technical assistance and providing legal information, the main tasks of the contact point include: computer data preservation; collection of evidence; the location of the suspects.

Therefore, in addition to the other forms of expedited cooperation provided for in this Protocol, the drafters were aware of the need to facilitate the ability of the Parties, in an emergency, to quickly obtain computer data stored in the possession or control of a service provider in the territory of another Party to be used in specific criminal investigations or proceedings, in accordance with the provisions of the Article 9 of the second additional protocol.

As noted in paragraphs 42 and 172 of this explanatory report to the second additional protocol, the need for maximum rapid cooperation may arise in a variety of emergency situations, such as immediately following a terrorist attack, a ransomware attack that can paralyze the hospital system, or when investigating email accounts used by kidnappers to issue demands and communicate with the victim's family (Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence. Explanatory Report, 2021, p. 71-72).

We note that the innovation of this second additional protocol lies in the elaboration of two articles that oblige all parties to provide, at least, specific channels for rapid cooperation in emergency situations: Article 9 and Article 10.

Article 9 allows Parties to cooperate to obtain computerized data in emergency situations using the 24/7 Network established by the Article 35 of the Council of Europe

Convention on Cybercrime as a channel (Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence. Explanatory Report, 2021, p. 67-69).

Article 10 of the second additional protocol is intended to provide an expedited fast-track procedure for requests for mutual assistance made in emergency situations. An emergency is defined in Article 3, paragraph 2 (c), and explained in related paragraphs 41 and 42 of the explanatory report to the second additional protocol (Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence. Explanatory Report, 2021, 41). Therefore, according to the Article 2(2)(c) "emergency" means "a situation in which there is a significant and imminent risk to the life or safety of any natural person".

As Article 10 of the second additional protocol is limited to emergency situations justifying such prompt action, it differs from Article 25 paragraph 3 of the Council of Europe Convention on Cybercrime, where requests for mutual assistance may be made by means of rapid communication in urgent circumstances which does not rise to the level of emergency as defined.

In other words, we note that the Article 25(3) of the Council of Europe Convention on Cybercrime has a wider scope than Article 10 of the second additional protocol in that, it covers situations not covered by Article 10, such as permanent but not imminent risks to the life or safety of persons, the potential destruction of evidence that may result from delay, a fast-approaching trial date, or other types of emergencies. While the mechanism in Article 25, paragraph 3, stipulates a faster method of submitting and responding to a request, the obligations in an emergency under the Article 10 of this protocol are significantly greater, that is, where there is a significant and imminent risk to the life or safety of an individual, the process should be further accelerated.

The use of the channel established in the Article 9 of the second additional protocol may have advantages over the emergency mutual assistance channel provided by the Article 10. For example, this channel has the advantage that no request for mutual assistance needs to be prepared in advance.

Considerable time may be required to prepare a prior request for mutual assistance, to translate it and to transmit it through internal channels to the requesting party's central authority for mutual assistance, which would not be necessary under Article 9 of the second additional protocol. Furthermore, once the requested party has received the request, if it needs to obtain additional information before it can provide assistance, the additional time that may be required for a mutual assistance request is more likely to slow down the execution of the request.

As provided in Article 5, paragraph 5, the section 5 relating to Articles 11 and 12, applies "where there is no mutual assistance treaty or arrangement based on uniform or reciprocal legislation in force between the requesting parties and those requested. The provisions of section 5 shall not apply where there is such a treaty or arrangement, except as provided in Article 12, paragraph 7. However, the parties concerned may agree to apply the provisions of section 5 instead, if the treaty or arrangement does not prohibit it".

We noted that the section 5 follows the approach of the Article 27 of the Council of Europe Convention on Cybercrime. Between some parties to this protocol, the subjects of Articles 11 and 12 are already covered by the terms of mutual assistance treaties, for example, the Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters (ETS No. 182) or the Agreement on Mutual Legal Assistance between the European Union and the United States of America. Mutual assistance treaties such as ETS no. 182, may also provide more details on the circumstances, conditions and procedures under which such cooperation may take place.

We emphasize that, although the drafters took into account these bilateral treaties or agreements, Articles 11 and 12 of the second additional protocol contain terms that differ from analogous provisions in other mutual assistance treaties.

Like Article 25 from the Council of Europe Convention on Cybercrime, the Article 27 is based on the idea that mutual legal assistance should be carried out through the application of relevant treaties and similar agreements, instead of exclusive reference to the Council of Europe Convention on Cybercrime (Moise, 2011, p. 354-355). The legislators of the Council of Europe Convention on Cybercrime decided not to establish a separate mandatory mutual legal assistance regime within the Convention.

If other legal instruments in the matter of mutual legal assistance are already in force, the provisions of Article 27 and Article 28 are not relevant in such a request. Only in those cases where other regulations are not applicable, Articles 27 and 28 provide a set of mechanisms that can be used to make requests for mutual legal assistance.

The most important aspects provided by the Article 27 of the Council of Europe Convention on Cybercrime are the following (Moise, 2011, 355): the obligation to establish an indicated contact point for requests for mutual legal assistance; the requirement for direct communication between contact points to avoid lengthy procedures; creation of a database with all contact points by the Secretary General of the Council of Europe.

In addition, the Article 27 defines the reservations in relation to requests for mutual legal assistance. States parties to the Council of Europe Convention on Cybercrime may refuse cooperation in particular: with regard to political crimes; and/or, if it is considered that the cooperation could harm the sovereignty, security, public order or other essential interests of the States Parties.

We note that the legislators of the Convention saw the need to allow the parties to refuse cooperation in certain cases on the one hand, but on the other hand they emphasized the fact that the parties should exercise the refusal of cooperation with restraint to avoid a conflict with the principles established before.

3. Conclusions

In this context it is important to highlight the fact that the second additional protocol like the Council of Europe Convention on Cybercrime, still does not define which authority should be responsible for the operation of the contact point in each member state. If a contact point in one Member State operates through an authority that has the

power to order data retention, and another contact point in another Member State makes a data retention request to it, then this measure can be put into application immediately by the requested point of contact.

Therefore, taking into account the analysis carried out, we find that the provisions of the second additional protocol in the matter of international cooperation are not always operational, because there are frequently encountered situations when other multilateral or bilateral instruments pre-existing the protocol have priority.

We are of the opinion that the second additional protocol, an important international legal instrument in the field of combating cybercrime alongside the Council of Europe Convention on Cybercrime, should be signed and ratified by as many states as possible around the world, especially non-European states, so that it becomes a tool with global applicability to allow rapid cooperation between member states in the field of cybercrime forensic investigation.

References

Moise, A. C. (2011). *Metodologia investigării criminalistice a infracțiunilor informatice* [The Forensic investigation methodology of cybercrimes]. Bucharest: Universul Juridic.

Council of Europe (2021). *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence*. *Explanatory Report*, Special edition dedicated to the drafters of the Protocol, Strasbourg, France, December 2021.

Council of Europe Treaty Series – No. 224 (2022). *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence*,Strasbourg, 12.05.2022.