www.coe.int/cybercrime

Version 25 November 2024

T-CY (2024)11

Preparation of a T-CY Guidance Note on Article 26
of the Convention on Cybercrime

"Spontaneous information" – Current practices of the use of Article 26

Background report prepared by the T-CY Secretariat and the
Cybercrime Programme Office of the Council of Europe

www.coe.int/cybercrime

Contents

Contact
Alexander SEGER
Executive Secretary
Cybercrime Convention Committee
Council of Europe
Strasbourg, France

Tel: +33-3-9021-4506
Mobile: +33-7-6099-2135
Email: cybercrime@coe.int

Disclaimer
This technical report does not necessarily reflect official positions of the Council of Europe or of Parties to the treaties referred to.

1 Introduction

At the 30th plenary meeting[1] in June 2024, the T-CY decided:

- To invite the T-CY Bureau to reflect on the need to draft a Guidance Note on "spontaneous information" (Article 26 of the Convention on Cybercrime (Budapest Convention)) while considering current practices of Parties.
- To therefore invite Parties to respond to a questionnaire to be circulated by the T-CY Secretariat and C-PROC seeking information on current practices by 1 September 2024.

On 25-26 September 2024, EUROJUST and the Cybercrime Programme Office of the Council of Europe (C-PROC) held a joint event on the topic of "spontaneous information" in The Hague (hereinafter referred to also as the "Workshop").[2] More than 70 experts from some 40 countries (EU members States and priority countries of C-PROC projects) participated in the Workshop.

The main aim of the Workshop was to:

- Identify current practices and learn from experience of countries on the use of spontaneous exchange of information.
- To address the key concepts of Article 26 of the Budapest Convention (BC) (such as "information" and "spontaneous").
- Find out whether and under what conditions the information obtained can be used as evidence.

This report contains the findings of the replies to the questionnaire[3] and the outcome of the Workshop in terms of the current practices of exchanging spontaneous information.

2 Overview of the use of Article 26 or similar provisions

2.1 Frequency of application

A positive trend indicated by the answers to the questionnaire and the discussion during the workshop is that almost all countries make use of spontaneous information mechanism. Very few do not use it at all so far. During the workshop, participants provided very valuable practical examples of the use of exchanging spontaneous information.

However, there are differences in the frequency of use. While some countries indicated that they use the mechanism frequently, a similar number of countries use it rather rarely.

Some countries also indicated that the frequency depends on the type of cooperation. One country stated that spontaneous exchange of information between judicial authorities is very sporadic, as this level is usually concerned with the exchange of evidence through formal international cooperation mechanisms, while spontaneous exchange of information is more common at the level of police-to-police cooperation.

[1] Held on 18-20 June 2024, in Strasbourg, France.
[2] The workshop was supported by the following C-PROC projects:
- GLACY-e;
- Octopus Project;
- CyberEast+;
- CyberSEE;
- CyberSouth+.

[3] Questionnaires were completed by 31 countries (replies received by 18 November 2024.

A smaller group of countries did not respond to this question of the questionnaire. Therefore, it may be useful to increase knowledge of how Article 26 can be used by Parties to the BC.

2.2 Statistics

Most of the countries do not keep data/statistics on spontaneous information provided or received, while some do. Others that do not keep such data separately, seem to be able to extract them from the national electronic case management system. At least one country indicated that it is preparing its system to be able to keep such data/statistics soon.

2.3 Use of bilateral or multilateral agreements or voluntary arrangements with other Parties that permit the spontaneous exchange of information

Countries have identified the following multilateral agreements as the legal basis for spontaneous information exchange, including at police level:

- Convention on Cybercrime;
- United Nations Convention against Transnational Organized Crime;
- United Nations Convention against Corruption;
- Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters;
- 2000 EU Mutual Legal Assistance Convention;
- Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime;
- Convention on Mutual Legal Assistance in Criminal Matters between the Member States of the Community of Portuguese Speaking Countries (CPLP).

Some countries also stated that they use bilateral agreements or voluntary arrangements with judicial authorities of other countries, where the spontaneous transmission of information is one of the stated objectives.

Another basis for cooperation mentioned by several countries is the Interinstitutional Cooperation Agreement between Ibero-American Prosecutors, which, among other things, regulates the use of spontaneous information exchange.

Some countries indicated that they also use other bilateral/multilateral agreements than those listed above providing for information exchange at police level.

2.4 Written procedures on how to transmit/receive spontaneous information

Most of the countries do not use any specific internal regulations or other guidelines and rely either on:

- direct application of the relevant provisions of multilateral conventions and agreements, or
- procedures contained in applicable provisions of their domestic legal framework (such as those contained in laws governing international cooperation in criminal matters).

However, a few countries indicated that they had issued specific guidelines (e.g. internal guidelines for prosecutors) or provided guidance on the spontaneous exchange of information on their authorities' websites.

Reference was also made to the following internationally adopted guidelines:

- Protocol for Action on the Spontaneous Transmission of Information developed within the Network of Anti-Drug Prosecutors of the Community of Portuguese-Speaking Countries;

- Guide for Use of the Inter-institutional Cooperation Agreement between the Public Prosecutor's Offices and Prosecutors members of Ibero-American Association of Public Prosecutors (AIAMP) ;
- Manual for the Exchange of Information developed within The Financial Action Task Force of Latin America (GAFILAT).

3 Legal provisions and concepts related to spontaneous information

3.1 Legal basis for spontaneous exchange of information

A number of countries rely on the direct application of relevant provisions of international instruments. Some countries indicated that the provisions of international instruments were directly applied to judicial cooperation, while spontaneous exchanges for police-to-police cooperation were governed by domestic law.

There are also countries that rely on the direct application of international instruments complemented by their domestic legal framework.

One country indicated that although the spontaneous information exchange is provided for in domestic law, where international treaties contain provisions that conflict with or complement domestic law, the treaty law prevails and applies automatically.

A larger group of countries relies on the application of domestic legal provisions for the exchange of spontaneous information. The applicable provisions can be found in specific laws on international cooperation in criminal matters (for judicial cooperation), police laws (for police-to-police cooperation), specific cybercrime legislation or financial transaction reporting.

A few countries indicated that provisions of bilateral instruments were the legal basis for such cooperation.

One country stated that it relied on case law and one country on the text of a guide based on Art. 26 of the BC.

One country stated that there was no legal basis for cooperation pending implementation into national law (although direct application of the applicable provisions of international instruments was not ruled out).

Most of these countries would apply the measure for the collection of electronic evidence of any offence, rather than for a limited list of offences. One country pointed out that it only uses the procedure in cases of sexual abuse and exploitation of children. Countries pointed out that other common uses of spontaneous information exchange concerned fraud, scams, money laundering, financial crime, etc.

3.2 The concept of “spontaneous”

Most of the countries that replied to the questionnaire stated that the concept of "spontaneous" was not defined in their domestic law.

However, some of these respondents indicated that although the term was not defined, it is understood to mean one or more of the following:

- information provided on a voluntary basis;
- proactively sharing information;

- information not previously requested by the receiving State;
- information provided without a letter rogatory;
- transfer of personal data from criminal investigations “without request”;
- on the own initiative of competent authorities;
- without a prior request from the receiving Party;
- unsolicited transmission of information to the authorities of another State;
- any type of information in general that has been obtained as part of operative investigative or criminal prosecution activities.

During the Workshop, the question was discussed whether an exchange that follows an initial exchange of spontaneous information and relates to the same case can still be considered spontaneous and whether such follow-up information can continue to be exchanged in the spontaneous exchange mode. A practical case demonstrated the usefulness of such exchanges. It was noted that if countries sharing information in this way agree among themselves on this approach, such sharing could continue to be considered to be part of the same spontaneous exchange.

It was also stated by others that some form of informal consultation may take place before and after the information is shared. It may also be discussed why in a particular case it is not appropriate to use the format of an MLA request and instead send the data under the spontaneous exchange regime. For more information, please see also section on follow-up.

3.3 The concept of “information” (within the context of international cooperation in criminal matters)

Most of the countries that replied to the questionnaire do not define the concept of "information" in their domestic law when referring to the sharing of information.

Some of them pointed out that although the term is not defined, the term " information" is used in relation to the following terms, concepts and interpretations:

- "element of proof" or "evidence";
- any information obtained in the course of criminal proceedings;
- definition of a private document;
- wide range of data, records, and evidence that could be shared or requested in the context of international criminal investigations and cooperation;
- the concept is interpreted in the general context of the collection and exchange of data necessary for the implementation of international cooperation in criminal matters;
- not defined but used in the context of describing various procedures for the internal application of forms of international judicial cooperation.

Few countries define the term “information” in their domestic law. The following examples of definitions were provided:

- text messages, data, voice recordings, sounds, databases, videos, signals, software, computer programs and codes including object codes and source codes;
- all data held by the competent law enforcement authorities which are available to the competent law enforcement authorities without the use of coercive procedural measures (this concept does not include information constituting a state secret);
- definition of personal data (e.g. name, address, date of birth, place of birth, age, etc.);
- knowledge that may be communicated in any form and which can include personal and/or non-personal data
- presentation of facts or concepts in an automated processing format, including software that enables an information system to function.

Furthermore, it was noted during the Workshop that whether what countries exchange was information and whether it becomes evidence depended on the subsequent procedures in the receiving country or the conditions imposed by the transmitting country which may limit the use of the information provided.

3.4 Article 26: a method of police-to-police cooperation for the sharing of information/intelligence vs judicial cooperation for the sharing of evidence?

Most countries indicated that they considered cooperation under Art. 26 of the BC to cover both police-to-police and judicial cooperation.

Several of these countries pointed out that the spontaneous exchange of information usually starts as police-to-police cooperation and becomes judicial cooperation when the information exchanged becomes part of formal legal proceedings and is used as evidence in court.

Fewer countries considered cooperation under Art. 26 of the BC as exclusively police-to-police cooperation and even fewer as exclusively cooperation between judicial authorities.

However, several countries (regardless of whether they consider the spontaneous exchange of information as police-to-police cooperation, judicial cooperation or both) stressed that further specific conditions must be met in order for information to be used as evidence in criminal proceedings, or to exclude the information from being used as evidence in criminal proceedings (see also other parts of this report).

4 Providing spontaneous information

4.1 Type of information that can be transmitted spontaneously

The responses to the questionnaire showed that countries may share a fairly wide range of information spontaneously.

On the basis of the replies, the most common reasons why countries spontaneously provide information to another country are:

- information may assist the receiving country in initiating or carrying out investigations or criminal proceedings;
- information may prevent crime from being perpetrated;
- information may lead to a request for mutual legal assistance by the receiving state;
- information being considered as relevant (including personal data).

In this context, one country during the Workshop referred to a practical case of the use of spontaneous exchange of information to prevent further crime. Article 26 of the BC was used as the legal basis for this exchange.

The following types of information that can be provided spontaneously were mentioned in replies by countries:

- police intelligence information (as investigative lead);
- information deriving from evidence gathered during a domestic investigation;
- crime reports;
- identity of perpetrators or victims or other information about the commission of an act;
- witness examination;
- incident reports, cybersecurity vulnerabilities and exploits;
- public information which has not involved violating fundamental rights in obtaining it;

- IP addresses, emails, social media accounts or instant messaging services linked to cyberattack;
- information related to bank account such as IBAN, analysed information of electronic communication, part of the victims' statements.

4.2 Channels and procedures used

Countries indicated that different types of authorities can decide whether information should be sent to another country. These may include law enforcement officials, prosecutors or judges. However, these authorities do not usually send the information directly themselves, but instead use another competent channel under their domestic law.

For police-to-police cooperation, countries rely on the use of the following channels:

- 24/7 contact points (such as those under Art. 35 of the BC);
- central authorities (national police authorities or relevant ministries such as the Ministry of Justice);
- other channels: INTERPOL, EUROPOL, Egmont group.

Some countries also indicated that, in the context of police-to-police cooperation, direct exchanges between police authorities could be used in some cases. One country indicated that a public prosecutor could be used as a channel for such exchanges.

With regard to judicial cooperation, countries referred to the use of the following channels:

- central authorities (cooperation through relevant ministries or general prosecutor's offices);
- 24/7 contact points;
- direct communication between the contact points of specialised networks (regional prosecution networks[4]);
- other channels: EUROJUST.

In some cases, judicial cooperation may involve direct exchanges between prosecutors or, less frequently, between judges. In this context, one country also pointed out that after the initial contact by central authorities, the judicial authorities involved may exchange further information directly, although coordination with the national central authority is recommended.

Two countries indicated that although diplomatic channels can be used for spontaneous information exchange, these are rather complementary to existing channels for judicial cooperation and that other channels allowing for more expeditious exchange should be preferred.

It was also noted during the Workshop that, depending on national laws, different authorities in the receiving country may be responsible for assessing how the information should be handled. It was pointed out that police officers and prosecutors may perhaps be in a better position to make this decision, whereas the judge has the final say when it comes to using the information as evidence in court.

4.3 Permission to use Information as evidence in criminal proceeding

The country providing the information does not have to impose any restrictions on the use of the information, and most countries indicated that the information could be used as evidence in the receiving country if the law of the receiving country allowed it.

[4] For example, communication between the contact points of the CiberRed (a network of prosecutors specialising in cybercrime among Ibero-American countries).

However, some conditions may be required/imposed by the transferring country (see the section below).

Another group of countries pointed out that it depends on a case-by-case basis. For example, the information may not be allowed to be used as evidence in criminal proceedings if it could jeopardise ongoing criminal proceedings in the transmitting country.

It was also pointed out that if the information was obtained through a channel hat was not considered as formal channel for the international cooperation, it could not be used as evidence in the receiving country. Several countries also specified that if the information was obtained through police-to-police cooperation, it could not be used as evidence in the receiving country and that the receiving country should send a formal MLA request in order to be able to use the information as evidence.

Some countries also stated that if the receiving country asks for permission to use the information as evidence, the sending country can give its consent.

A small number of countries indicated that they do not allow or usually do not allow the information to be used as evidence in criminal proceedings. The most common reason given was that the purpose of providing information is to enable the receiving country to prepare a request for mutual legal assistance, and not to use the information subsequently as evidence.

4.4 Conditions typically required or impose on the receiving Party

A large group of countries usually require several conditions to be met that would determine how the receiving could use the information. These conditions may be required by law, by internal standard operating procedures/implementation guides, or by the competent authorities of the transmitting country.

Countries reported that they impose or require the following conditions on receiving countries:

- confidentiality of data;
- purpose limitation - only to be used for the investigation of the case for which it was provided;
- not to transfer the information to another country without prior consent;
- dual criminality;
- only for initiating a procedure or making a request for mutual legal assistance;
- data protection;
- reciprocity;
- to use the information only for intelligence purposes and not as evidence;
- to ensure appropriate and lawful use of the information;
- to provide notification about further use/follow-up how the information was used;
- information can be used only to detect the commission of cybercrime;
- not to be used for the purposes of procedures that violate fundamental rights and guarantees;
- conditions provided in multilateral or bilateral treaties;
- other conditions as specified by authorities/depends on the case.

Only two countries indicated that they do not usually impose or require any conditions on the receiving country.

5 Receiving spontaneous information

5.1 Information received through the spontaneous exchange as evidence without the need for issuing an MLA request?

While more countries can use information obtained through spontaneous exchange as evidence, this may sometimes depend on several circumstances:

- the nature/type of the information received;
- legislation or decision of the country providing information;
- if the collection does not exclude its admissibility due to incompliance with national fair trial safeguards;
- domestic legislation or decision of domestic authorities competent in the criminal proceedings (e. g. the court conducting the criminal proceedings);
- the channel used to send the information (central authority or within the framework of a JIT);
- prior consent or certification given by the providing country.

Less than half of the countries stated that information obtained through spontaneous exchanges could not be used as evidence (see also the following section on restrictions).

It was also stated that the admissibility of evidence should be distinguished from the free assessment of evidence in court, as these are two different concepts.

5.2 Restrictions

Of those countries that reported that there were restrictions preventing them from using the information as evidence in criminal proceedings, the most common reason given was that the information could not be used as evidence in criminal proceedings because:

- their domestic laws do not regulate how these countries should handle spontaneously received information;
- in case it is regulated in the domestic law, the information obtained through spontaneous exchanges cannot be used as evidence; it must go through mutual legal assistance procedures in order to be used as evidence.

Few countries stated that the restriction depends on jurisprudence or practice.

A number of countries have indicated that there are no restrictions in their national legislation on the use of spontaneous information as evidence.

Several countries stated that it depends on the nature of the information received whether it can be used as evidence. The following circumstances were mentioned in the countries' replies:

- if intelligence information (received through police-to-police cooperation), it cannot be used as evidence;
- Information can be used only for a specific purpose such as to prevent a direct and serious threat to public safety;
- Information is excluded as evidence if it is largely hearsay and no original source can be identified to confirm its veracity;
- sensitivity of information (for example, in the case of content data, one country indicated that it assesses whether such data was obtained under judicial supervision. Another country specified that there must also be judicial oversight of the collection of data covered, for example, by banking secrecy).

Almost the same number of countries indicated that the nature of the information was not a determining factor for restrictions on its use as evidence in criminal proceedings. A first group of these countries can use any type of information as evidence, regardless of its nature.

Another group of countries, which can only use information obtained through mutual legal assistance as evidence, require this more formal form of cooperation for all types of information, also regardless of their nature.

One country specified that its competent authorities have discretion to decide how to deal with spontaneously received information and that it is not the nature of the information that matters.

One country pointed out that, although there is no difference in nature per se, when only summary information is provided, the underlying documents (e.g. bank documents, etc.) are usually obtained subsequently for verification as part of the free evaluation of evidence.

There were countries that indicated that the other factors determine whether restrictions on the use of information as evidence should be applied:

- the channel used to transmit of the information (however, one country pointed out that even if a formal channel is required for the information to be used as evidence, a final judicial decision from another country obtained through a spontaneous exchange of information could be recognised incidentally and lead to the discontinuance of criminal proceedings in the receiving State, even if the information is not subsequently transmitted through mutual legal assistance).
- prior notice by the transmitting country.

The Workshop also discussed the possibility of using information obtained in a manner contrary to the law of the receiving country. While some countries stated that information obtained in this way could not be used as evidence[5], others stated that their domestic laws did not exclude such a possibility. However, some specified that the information would not be used as evidence in cases where it had been obtained through serious violations of fundamental rights, such as torture (Art. 3 ECHR).

5.3 Follow-up to the authorities of another country from whom the information was obtained

Countries indicated that they provide feedback/follow up with the authorities from which the information was received or that they provide feedback depending on the specific situation. The following responses were received from countries:

- follow-up with the authorities from which the information was obtained, if specifically requested by those authorities;
- If, in the course of the operation, information is found which may be relevant to the other country;
- whether a criminal investigation (prosecution) has been initiated or declined as a result of the information received;
- whether the information has led to or is useful for further investigation;
- If information is to be used as evidence, "follow up" through a formal mutual legal assistance request;
- follow-up information may be provided on the progress of the investigation;
- focus on maintaining extremely close channels of communication;
- no formal obligation, but feedback sometimes provided;

[5] However, it was noted that even such information could be used as a basis for developing admissible evidence through further investigation.

- feedback is usually provided through informal channels, including email and discussions with the countries involved;
- where further cooperation is required;
- on how the information has been used or any findings in the case that may be useful to the other country;
- based on reciprocity;
- feedback if some elements of the information are missing;
- any follow-up in accordance with normal practice;
- feedback by sharing the final decision (final judgment).

6 Conclusions

The replies to the questionnaire and the discussions in the Workshop showed that there are different and heterogeneous practices in relation to the concept of spontaneous information exchange. This concerns the way the information is transmitted (authorities sending the information, channels to be used, etc.) and the way the information is used by the receiving country (as noticia criminis, as evidence, etc.).

However, it appears that these differences in the countries' approaches to spontaneous information exchange do not prevent Parties from cooperating successfully. The group exercise during the Workshop was a good example of this finding. In the exercise, each group was composed of experts from different regions of the world, with different legal systems and different understandings of spontaneous information exchange. Each group was invited to work together to find common approaches to solving the scenario given. Despite these differences, each group was able to find a solution that led to a spontaneous exchange of information in the given case.

The following additional conclusions can be drawn based on the responses to the questionnaire and the Workshop:

- In most cases, traditional forms of international cooperation are not effective, and more efficient measures should be considered instead.

- Article 26 of the BC provides for such a measure by providing a legal basis for spontaneous exchange of information between the Parties to the BC. This can be particularly helpful for countries that do not have such a measure in their domestic law but can directly apply international treaty provisions.

- Most countries understand cooperation under Art. 26 of the BC to cover both police and judicial cooperation.

- Most of the countries apply the spontaneous exchange of information to the collection of electronic evidence of any criminal offence and do not limit it to a list of criminal offences.

- The concepts of “spontaneous” and “information” are typically not defined by domestic laws.

- Countries share a wide range of information. The concept of information is thus understood rather broadly.

- Regulating the admissibility of the outcome of the exchange of evidence under Article 26 of the BC in domestic law is key.

- Some countries have already started to explore avenues of how Article 26 of the BC could be applied and integrated in domestic legal reforms underway or envisaged.

- Cooperation under Article 26 of the BC can bring added value to international cooperation on cybercrime and electronic evidence overall and could be a starting point before other tools/mechanism are used.

- There is a clear need to improve knowledge and provide further assistance/guidance to Parties on how to apply and use Article 26.

7 Annex

List of countries that replied to the questionnaire:

Albania, Andorra, Bosnia and Herzegovina, Brazil, Cabo Verde, Cameroon, Colombia, Costa Rica, Fiji, Germany, Ghana, Japan, Kosovo*, Liechtenstein, Lithuania, Mauritius, Moldova (the Republic of), Montenegro, North Macedonia, Panama, Peru, Philippines, Poland, Portugal, Romania, Serbia, Spain, Tunisia, Türkyie, United Kingdom of Great Britain and Northern Ireland, United States of America.

List of participating countries in the Workshop (the Hague, 25-26 September 2024)[6]:

Albania, Algeria, Argentina, Armenia, Belgium, Benin, Bosnia and Herzegovina, Brazil, Cameroon, Cape Verde, Chile, Colombia, Costa Rica, Cote d'Ivoire, Dominican Republic, Ecuador, Georgia, Ghana, Jordan, Kiribati, Kosovo*, Lebanon, Mauritius, Moldova, Montenegro, Morocco, Nigeria, North Macedonia, Panama, Paraguay, Peru, Philippines, Senegal, Serbia, Sierra Leone, Spain, Sri Lanka, Sweden, Tunisia, Ukraine, United States of America, Vanuatu.

Spontaneous Information Sharing Art. 26 Budapest Convention Case Study[7]

* Throughout this text, all reference to Kosovo, whether to the territory, institutions or population, shall be understood in full compliance with UN Security Council Resolution 1244 and without prejudice to the status of Kosovo.

[6] The outline and the agenda are available for download here.

[7] The case study is available for download here.