www.coe.int/cybercrime

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 25 June 2025 T-CY(2025)3

Cybercrime Convention Committee (T-CY)

T-CY Guidance Note #14
Spontaneous information
(Article 26 Convention on Cybercrime)

Reviewed by the T-CY 32 (2-3 June 2025)
and adopted through silent procedure on 25 June 2025

Content

Contact

Secretariat of the Cybercrime Convention Committee
Directorate General of Human Rights and Rule of Law
Council of Europe, Strasbourg, France

Email T-CY.secretariat@coe.int
www.coe.int

1 Introduction

The Cybercrime Convention Committee (T-CY) at its 8th Plenary (December 2012) decided to issue Guidance Notes aimed at facilitating the effective use and implementation of the Convention on Cybercrime, also in the light of legal, policy and technological developments.[1]

Guidance Notes represent the common understanding of the Parties to this treaty regarding the use of the Convention.

Criminal justice authorities in one jurisdiction may possess information that they believe could assist another Party in a criminal investigation or proceeding, but in some instances, the investigating Party may be unaware of the existence of that information. Article 26 of the Convention provides a legal basis for forwarding such information to the other Party without a prior request.

The importance of Article 26 has increased over time, including within the context of investigations involving the dark web or the collection of large amounts of data obtained from communications. At the same time, not all Parties make use of all the possibilities of this provision in a consistent manner.

The T-CY, therefore, decided that guidance on Article 26 drawing on current practices of Parties in the application of Article 26 would be of value and permit Parties to take full advantage of the potential of the Convention with respect to spontaneous information.

The present note thus addresses key aspects of (a) the transfer of spontaneous information and (b) its use in the receiving Party when obtained on the basis of Article 26, including whether or not the information received may be used as evidence when received on the basis of this Article.

This note is also based on the results of the replies to the questionnaire[2] received from Parties by January 2025, the outcome of a joint event on "spontaneous information" organised in co-operation with Eurojust in The Hague, a background report[3] and discussions held at Octopus Conference in Bucharest 2023[4].

2 Article 26 Convention on Cybercrime

Text of the provision:

> **Article 26 – Spontaneous information**
>
> 1 A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences

[1] See the mandate of the T-CY (Article 46 Convention on Cybercrime).

[2] Questionnaire on practices by Parties to the Convention was sent to T-CY Representatives in July 2024.

[3] T-CY Secretariat and the Cybercrime Programme Office of the Council of Europe "Spontaneous information" – Current practices of the use of Article 26, presented at the 31st T-CY Plenary (11-12 December 2024) and updated in May 2025 (document T-CY (2024)11rev).

[4] The Octopus Conference 2023 (13 December 2023) featured a workshop on spontaneous information sharing.

established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter.

2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.

Extract of the Explanatory Report:

260. This article is derived from provisions in earlier Council of Europe instruments, such as Article 10 of the Convention on the Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (ETS N° 141) and Article 28 of the Criminal Law Convention on Corruption (ETS N° 173). More and more frequently, a Party possesses valuable information that it believes may assist another Party in a criminal investigation or proceeding, and which the Party conducting the investigation or proceeding is not aware exists. In such cases, no request for mutual assistance will be forthcoming. Paragraph 1 empowers the State in possession of the information to forward it to the other State without a prior request. The provision was thought useful because, under the laws of some States, such a positive grant of legal authority is needed in order to provide assistance in the absence of a request. A Party is not obligated to spontaneously forward information to another Party; it may exercise its discretion in light of the circumstances of the case at hand. Moreover, the spontaneous disclosure of information does not preclude the disclosing Party, if it has jurisdiction, from investigating or instituting proceedings in relation to the facts disclosed.

261. Paragraph 2 addresses the fact that in some circumstances, a Party will only forward information spontaneously if sensitive information will be kept confidential or other conditions can be imposed on the use of information. In particular, confidentiality will be an important consideration in cases in which important interests of the providing State may be endangered should the information be made public, e.g., where there is a need to protect the identity of a means of collecting the information or the fact that a criminal group is being investigated. If advance inquiry reveals that the receiving Party cannot comply with a condition sought by the providing Party (for example, where it cannot comply with a condition of confidentiality because the information is needed as evidence at a public trial), the receiving Party shall advise the providing Party, which then has the option of not providing the information. If the receiving Party agrees to the condition, however, it must honour it. It is foreseen that conditions imposed under this article would be consistent with those that could be imposed by the providing Party pursuant to a request for mutual assistance from the receiving Party.

3 T-CY interpretation of Article 26 Convention on Cybercrime

3.1 The scope of Article 26, general considerations and safeguards

3.1.1 Discretionary nature of Article 26

Article 26 provides a legal basis for a Party to transmit to another Party information obtained in the course of its own investigation.

The provision leaves it to the discretion of a Party ("a Party may (…)") whether to forward the information to another Party. A Party is not obligated to spontaneously forward information to another Party; it may exercise its discretion in the light of the circumstances of the case at hand.

3.1.2 On the concepts of "spontaneous" and "without prior request"

The concept of "spontaneous" implies that the Party transmits information obtained in the course of its own domestic investigations voluntarily or on its own initiative, without a prior request for mutual assistance from another Party.

This does not exclude the possibility of informal consultations between the Parties prior to the exchange of spontaneous information. The consultations may, for example, relate to specific conditions that the providing Party may wish to impose, or to questions such as the communication of reasons why, in a particular case, it would be preferable to transmit the data under Article 26 rather than through mutual assistance procedures.

At the same time, the Parties may also consider it useful to have a follow-up consultation after a Party has received information transmitted through a spontaneous exchange. Questionnaire results showed that Parties often engaged in subsequent consultations, after the initial disclosure to discuss the details and the need for further disclosure of spontaneous information. If the Parties so agree, they may continue to exchange future information related to the case that triggered the initial transmission, also pursuant to Article 26. If deemed more appropriate, the Parties may decide to exchange future information through mutual assistance procedures.

3.1.3 On the concept of "information"

The providing Party may forward any relevant information obtained in the course of its own investigation. "Information" in this context is understood broadly and may take the form of computer data or any other form.

Parties can transmit different types of information under the procedure provided for in Article 26. In their responses to the questionnaire, Parties included the following examples:

- information gathered in the course of a domestic investigation;
- police intelligence information;
- crime reports;
- identity of perpetrators or victims or other information about the commission of an act;
- witness examination reports;
- incident reports,
- cybersecurity vulnerabilities and exploits;
- Internet Protocol (IP) addresses, emails, social media accounts or instant messaging services associated with a cyber-attack;
- bank account-related information such as IBAN or victims' bank statements (or parts thereof);
- registration and other non-content records associated with accounts used in connection with the crimes under investigation;
- contents of communications.

The information transmitted may be in the form of computer data or in any other form as may be determined by the Party transmitting the information.

3.1.4 On the concepts of "initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention" and "might lead to a request for co-operation by that Party under this chapter"

A Party may consider spontaneously forwarding information obtained within the framework of its own investigations to another Party under the following conditions:

- such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention; or
- such information might lead to a request for co-operation by that Party under this chapter.

Article 23[5], which sets out the general principles of international co-operation, makes it clear that co-operation is not only possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, but also for the collection of evidence in electronic form of any criminal offence:

> Article 23 – General principles relating to international co-operation
> The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through the application of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

This broad scope also applies to Article 26. In practice, Parties provide spontaneous information under Article 26 in relation to any criminal offence; they do not limit it to offences related to computer systems or data.

In addition, Parties provide information spontaneously for various purposes. These include information that may assist the receiving State in initiating or conducting investigations or criminal proceedings, information that may prevent the commission of an offence, or information that may lead to a request for mutual legal assistance by the receiving State. In general, Parties provide any information when they consider it relevant. It is up to the receiving Party to decide what to do with the information received, subject to any conditions imposed by the Party that provided the information.

3.1.5 On the concept of "within the limits of its domestic law"

In deciding whether to forward information to another Party, a Party shall be guided by "the limits of its domestic law". Depending on their domestic laws, Parties have the discretion to provide for such limits. These limits include conditions and safeguards in accordance with Article 15 of the Convention[6].

[5] Both Article 23 and 26 are under the same Chapter 3 of the Convention, making Article 23 fully applicable to Article 26.

[6] Including confidential/restricted information due to legal privileges, immunities and witness protection, etc. based on paragraph 147 of the Explanatory report to the Convention.

It is also assumed that both the providing and receiving Parties respect the rule of law and human rights principles in line with Article 15 of the Convention.

> Article 15 – Conditions and safeguards
> 1 – Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights against pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.
> 2 – Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, inter alia, include judicial or other independent supervision,
> grounds justifying application, and limitation of the scope and the duration of such power or procedure.
> 3 - To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.

3.2 Authorities deemed competent in accordance with Article 26

Some provisions of Chapter III of the Convention (for example, Article 24 on Extradition or Article 27 on Procedures pertaining to mutual assistance requests in the absence of applicable international agreements) require Parties to designate authorities for these specific types of co-operation.

Article 26 does not contain such a requirement and refers to a "Party". The provision leaves it to the discretion of a Party to decide which authorities it considers competent to transmit information to another Party.

The practice of the Parties to the Convention indicates a wide range of authorities transmitting the information. These include police authorities, prosecutors and judges. In some cases, the sharing of spontaneous information may begin as police-to-police co-operation[7] and then turn into judicial co-operation when the information shared becomes part of formal legal proceedings and is used as evidence in court.

Based on questionnaire results, some Parties also use direct communication between relevant authorities. What may start as an initial contact between central authorities can further develop into direct exchanges. However, some Parties prefer communication/co-ordination through central authorities, which can provide their domestic authorities with the necessary guidance on applicable laws and conditions.

Questionnaire results also revealed that the Parties use various national channels (for example, 24/7 Network of points of contact[8] or central authorities) for transmitting information under Article 26 or international channels (for example, INTERPOL, EUROJUST, EUROPOL) for transmitting such information.

[7] However, further specific conditions may be required by some Parties for information obtained through police co-operation to be used as evidence in criminal proceedings in the receiving Party.

[8] See Article 35 Budapest Convention on Cybercrime.

3.3 Confidentiality and other conditions

3.3.1 Confidentiality

According to Article 26.2 of the Convention, a Party may make the spontaneous provision of information subject to a condition that sensitive information be kept confidential or that other conditions be imposed on the use of the information, including for example time boundaries, i.e. not to use the information as such before the criminal file advances to court in the providing Party.

Confidentiality is one of the conditions most frequently imposed by Parties to ensure confidentiality of the providing Party's investigation or proceeding.

Confidentiality will be "an important consideration in cases in which important interests of the providing Party may be endangered should the information be made public, e.g., where there is a need to protect the identity of a means of collecting the information or the fact that a criminal group is being investigated"(paragraph 261 Explanatory Report to the Convention).

3.3.2 Other conditions

The Parties may make the spontaneous disclosure of information subject to additional conditions, which may be determined on a case-by-case basis.

While the Parties may impose a wide variety of conditions under this article, it is foreseen that conditions imposed under this article would be consistent with those conditions that could be imposed by the providing Party in response to a request for mutual assistance from the receiving Party (paragraph 261 Explanatory Report to the Convention).

Parties' questionnaire responses and feedback of the Parties in the drafting process of this Guidance Note revealed that conditions may include, for example, where not otherwise in conflict with agreements or arrangements between the Parties concerned:

- do not use the information provided for any purpose other than that for which it was provided (if the purpose is specified);
- do not transfer the information to another country without prior consent;
- use the information only for initiating a procedure or making a future request for mutual legal assistance;
- comply with data protection conditions;
- reciprocity: guarantee that in the event of a similar future case, if the Party has obtained relevant information obtained within the framework of its own investigations, it will make all reasonable efforts to apply the procedure set out in Article 26 and forward the relevant information to the Party that imposed the prior reciprocity condition;
- do not use the information as evidence in criminal proceedings;
- ensure appropriate and lawful use of the information;
- provide notification about further use/follow-up on how the information was used;
- use the information only to investigate the commission of a crime and in criminal proceedings;
- notify the providing Party, or obtain permission from the providing Party, before any use that might result in the information becoming public;
- do not use the information for purposes of procedures that violate fundamental rights and guarantees;
- use the information pursuant to conditions provided in multilateral or bilateral treaties;

- use the information pursuant to other conditions as specified by authorities/ depending on the case;
- an anonymity clause: except in very exceptional circumstances, to be determined in accordance with the domestic law of the providing Party, such a Party will not provide information on the identity of investigating officers and/or honor any requests to take statement from the investigating officers, either in a hearing in court or elsewhere.

It should be noted, however, that under Article 26, the imposition of conditions is not mandatory and the providing Party may decide not to impose conditions on the use of the information in the receiving Party if it does not consider them necessary in a particular case. The decision whether and under what conditions to disclose the information is at the discretion of the providing Party.

3.3.3 Use of information as evidence in criminal proceedings in the receiving Party

The providing Party may make the disclosure of information subject to the condition that such information is not used as evidence in criminal proceedings in the receiving Party. Alternatively, the disclosing Party may attach other appropriate conditions, which, if met, will permit the use of the information as evidence in the receiving Party to the extent consistent with its domestic law. An example of such a condition would be the requirement imposed on the receiving Party to seek and obtain the information shared under Article 26 also through a mutual assistance procedure before it may be used as evidence in criminal proceedings in the receiving Party.

However, if no such conditions are imposed, the receiving Party may use the information as evidence in criminal proceedings to the extent consistent with its domestic law. This approach is in line with the Convention.

In some Parties, the domestic law permits the use of spontaneous information received as evidence in criminal proceedings if this is in accordance with the domestic law of the providing Party or such Party has provided its authorisation or consent. In the event of any ambiguity, the Parties usually resort to consultation.

Article 26 does not contain any rules on the admissibility of evidence and the T-CY considers that this is a matter for domestic law. Consultation between the Parties may reduce the risk that the information transferred is inadmissible in the receiving Party.

It should also be noted that the providing Party cannot oblige the receiving Party to use the information as evidence in the latter's criminal proceedings. There may be various conditions and restrictions in the domestic law of the receiving Party that are relevant to the type of information that can be used as electronic evidence in its criminal proceedings. The domestic law of some Parties may exclude spontaneously received information from being used as evidence in criminal proceedings for example, in the following cases:

- information was obtained through a channel or from an authority which the domestic law does not deem as competent for evidence sharing (for example, information obtained through police-to-police co-operation);
- information was obtained in a manner inconsistent with the domestic law governing such obtaining in the receiving Party;
- information can only be used for a specific purpose, such as preventing an imminent and serious threat to public security;
- information is largely hearsay and no original source can be identified to confirm its veracity or authenticity;

– information is of heightened sensitivity (for example, different procedures are required for more sensitive types of data such as content data or data related to bank secrecy).

Therefore, it may benefit both Parties to consult about how the information will be spontaneously shared in order to maximize the potential for its use without the need for additional requests or procedures. However, if the receiving Party is required under its domestic law to obtain the information by other means in order to be able to use it as evidence in criminal proceedings, such as by obtaining it through a mutual legal assistance procedure from the officially designated central authority, the Party that spontaneously provided the information should respect those requirements. Such a Party should not refuse to execute a subsequent request for mutual assistance on the sole ground that it had already provided the information through spontaneous disclosure. In addition, particularly in circumstances where a subsequent mutual legal assistance request is anticipated, it may be valuable to clearly document exactly what information was previously shared pursuant to Article 26 (for example, by use of zipped files and hash values), so that this data can be easily re-produced by the providing Party in response to the formal mutual legal assistance request.

3.4 Consultation and follow-up

If the receiving Party cannot comply with a condition sought by the providing Party (for example, where it cannot comply with a condition of confidentiality because the information is needed as evidence at a public trial in the receiving Party), the receiving Party shall advise the providing Party, which then has the option of not providing the information. If the receiving Party agrees to the condition, however, it must honour it (paragraph 261 Explanatory Report to the Convention).

Article 26 thus provides for the possibility of consultation between the Parties when it comes to informing the providing Party that a condition cannot be complied with.

However, such consultation may also be useful in cases where no specific condition has been imposed. For example, it may serve to determine whether the specific information provided spontaneously may be used as evidence in criminal proceedings in the receiving Party, if this was unclear at the time the information was provided.

In addition, as good practice, many Parties use such consultations to follow up with the Parties from which the information was obtained, in order to update that Party on how the information has been handled.

This is useful for maintaining close co-operation with another Party. Such follow-up may be provided when expressly requested by the Party providing spontaneous information but is not limited only to those cases.

Practice has shown that follow-up with the Party that provided the information can be useful in the following situations:

– in the course of an investigation initiated or carried out on the basis of spontaneously provided information, new information is obtained which may be relevant to the providing Party or to another Party;
– whether a criminal investigation (prosecution) has been initiated or declined based on the information obtained;
– whether the information has led to or is useful for further investigation and what the progress of the investigation is;

- where further co-operation is needed because some elements of the information are missing;
- when the final decision (final judgment) is given by the court.

Unless requested as a specific condition by the providing Party, it is up to the Party receiving spontaneous information to determine whether and in what cases a follow-up will be provided.

Practice has also shown that the Parties also use informal channels for follow-up purposes, including the use of oral or electronic communication.

3.5 Examples of the use of spontaneous information

- The authorities of Party 1 investigating an online forum for the sharing of child sexual exploitation and abuse materials discover that a member of this forum is communicating from an Internet Protocol address in Party 2. Party 1 authorities may use Article 26 to share this information with the authorities of Party 2, who may then initiate their own investigation of that member. While this information is shared by the authorities of Party 1 without a request for mutual assistance, the receiving Party 2 may decide to follow up with a request for mutual assistance if that is required by its domestic law in order to make use of the information as evidence in subsequent criminal proceedings.

- Through their investigations, the authorities of a Party have retrieved a very large amount of data related to communications between offenders from multiple jurisdictions, including offenders in other Parties. They may use Article 26 to share this information with the authorities of those other Parties – without requests for mutual assistance – who may then initiate their own investigations.

- The authorities of a Party receive a notice from a legal person in their territory regarding illegal access and data interference, having identified a significant loss of data that may indicate ransomware preparation. Following the investigation, they found out that the suspect was from another jurisdiction from where the attacks came from. Sharing information through Article 26 is an important measure to allow the authorities of the second Party to start their own investigation and stop the criminal activity.

- The authorities of a Party are investigating a case of computer-related fraud involving offenders and victims, including in multiple other Parties' jurisdictions, whose financial credentials have been compromised. The sharing of spontaneous information with the authorities of those other Parties may permit them to initiate their own investigations and to identify victims in their territory. At the same time, a Party may, when providing spontaneous information, request the receiving Party to provide a follow-up if the receiving Party has any information that may be useful for criminal investigations or proceedings in the Party providing spontaneous information.

- Article 26 may serve as a particularly useful and efficient tool for the sharing of spontaneous information indicating a significant and imminent risk to the life or safety of any natural person[9] in another Party. Such emergencies may include acts of terrorism, kidnapping or the ongoing sexual exploitation and abuse of children. The sharing of spontaneous information may help to identify and save victims of serious crimes. The

[9] Defined as "emergency" in Article 3.2.c of the Second Additional Protocol to the Convention on Cybercrime (CETS 224).

Party sharing the information may, for example, impose the condition that the information may only be used to address an emergency.

4 T-CY statement

The T-CY agrees that the above represents the common understanding of the Parties as to the scope and elements of Article 26 of the Convention on spontaneous information.

Article 26 is an affirmative legal basis for a Party to share information that it has obtained within its own investigation to another Party without a prior request for mutual assistance, when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings or that it might lead to a request for co-operation by that Party. The receiving Party may use the information as evidence in criminal proceedings, unless this is excluded by conditions imposed by the providing Party or is contrary to the domestic law of the receiving Party.

Given the benefits that Article 26 may provide, Parties are encouraged to consider how the procedure of "spontaneous information" under this article can be used effectively by their authorities.