UNITED NATIONS CONVENTION AGAINST CYBERCRIME

Last update: 04/07/2025

1. BACKGROUND

On 24 December 2024, the United Nations (UN) General Assembly (GA) adopted the *United Nations Convention against Cybercrime*[1] (UNCC), subtitled Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes.

The UNCC will be open for signature and accession to 193 countries that are members of the UN.[2] It will enter into force once forty States have become Parties.

The UNCC aims at:

- Promoting and strengthening **measures to prevent and combat cybercrime** more efficiently and effectively;
- Promoting, facilitating and strengthening **international cooperation** in preventing and combating cybercrime; and
- Promoting, facilitating and supporting **technical assistance and capacity-building** to prevent and combat cybercrime, in particular for the benefit of developing countries.

The UNCC has been largely inspired by the Council of Europe *Convention on Cybercrime* (also known as the Budapest Convention), which entered into force in 2004, becoming the first international treaty to focus explicitly on cybercrime and electronic evidence.[3]

ADDITIONAL RESOURCES ON SIRIUS

A review of the Budapest Convention and its Second Additional Protocol are available on the SIRIUS platform, as well as on the SIRIUS subpage on Eurojust's website.

2. SCOPE

As regards scope, the UNCC offers a broad institutional and global cooperation legal framework, covering a range of criminal offences and procedural powers related to cybercrime.

A- LEGAL REGIME COVERED

The UNCC covers a range of cybercrime-related topics. While it largely follows the provisions of the Budapest Convention, it goes beyond the scope of the existing legal instruments in some parts, especially in relation to its capacity-building provisions.

Providing a comprehensive global legal framework on cybercrime and gathering of electronic evidence, the UNCC is divided in 9 chapters:

[1] A/RES/79/243, Resolution adopted by the General Assembly on 24 December 2024.

[2] It will be open for signature at a signing ceremony in Hanoi, Viet Nam, on 25 October 2025 and thereafter at UN Headquarters in New York until 31 December 2026.

[3] A side-by-side analysis of the two international legal frameworks is available here. Kenneth Propp and DeBrae Kennedy-Mayo, From Budapest to Hanoi: Comparing the Council of Europe and United Nations Cybercrime Conventions, May 2025.

The Sirius Project has received funding from the European Commission's Service for Foreign Policy Instruments (FPI) under contribution agreement NDICI/2024/700002618.

- Chapter I: General provisions
- Chapter II: Criminalization
- Chapter III: Jurisdiction
- Chapter IV: Procedural measures and law enforcement
- Chapter V: International cooperation
- Chapter VI: Preventive measures
- Chapter VII: Technical assistance and information exchange
- Chapter VIII: Mechanism of implementation
- Chapter IX: Final provisions

The most important parts of the Convention, which are also found in the legal regime covered by the Budapest Convention, are presented below,

Crimes (Ch. II)	**Procedural measures** (Ch. IV)	**International cooperation tools** (Ch. V)
- Illegal access - Illegal interception - Interference with electronic data - Interference with an ICT system - Misuse of devices - ICT system-related forgery ICT system-related theft or fraud - Offences related to online child sexual abuse or child sexual exploitation material - Solicitation or grooming for the purpose of committing a sexual offence against a child - Non-consensual dissemination of intimate images - Laundering of proceeds of crime	- Expedited preservation of stored electronic data - Expedited preservation and partial disclosure of traffic data - Production order - Search and seizure of stored electronic data - Real-time collection of traffic data - Interception of content data - Freezing, seizure and confiscation of the proceeds of crime - Establishment of criminal record - Protection of witnesses - Assistance to and protection of victims	- Extradition - Transfer of sentenced persons - Transfer of criminal proceedings - 24/7 network - International cooperation for the purposes of expedited preservation of stored electronic data - International cooperation for the purpose of expedited disclosure of preserved traffic data - Mutual legal assistance (MLA) in accessing stored electronic data - MLA in the real-time collection of traffic data - MLA in the interception of content data - Law enforcement cooperation - Joint investigations - Mechanisms for the recovers of property through international cooperation in confiscation - International cooperation for the purposes of confiscation - Special cooperation - Return and disposal of confiscated proceeds of crime or property

Figure 1 – Areas covered by the UNCC

B- DATA COVERED

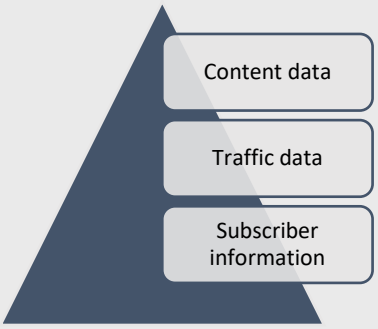

Figure 2 – Data categorisation in the UNCC

The UNCC introduces a new term "**electronic data**[4]" and defines it as any representation of facts, information or concepts in a form suitable for processing in an information and communications technology system, including

[4] Budapest Convention, for example, consistently employs the term "computer data".

a program suitable to cause an information and communications technology system to perform a function (Article 2(b)).

Mirroring the data categorisation set out in the Budapest Convention, the electronic data covered by the UNCC is divided into three categories:

- **subscriber information**,
- **traffic data**, and
- **content data**.

Subscriber information (Article 2(f) of the UNCC)

Any information that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:

(i) The type of communications service used, the technical provisions related thereto and the period of service;

(ii) The subscriber's identity, postal or geographical address, telephone or other access number, billing or payment information, available on the basis of the service agreement or arrangement;

(iii) Any other information on the site of the installation of communications equipment, available on the basis of the service agreement or arrangement.

Traffic data (Article 2(c) of the UNCC)

Any electronic data relating to a communication by means of an information and communications technology system, generated by an information and communications technology system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration or type of underlying service.

Content data (Article 2(d) of the UNCC)

Any electronic data, other than subscriber information or traffic data, relating to the substance of the data transferred by an information and communications technology system, including, but not limited to, images, text messages, voice messages, audio recordings and video recordings.

The electronic data covered by the UNCC may exist in two forms, in particular **stored data** or **data in the process of communication** (real-time data).

The **applicability of procedures** to a particular type or form of electronic data **depends on the nature and form of the data and the nature of the procedure**, as specifically described by each measure provided for in the UNCC.

C- SUBSTANTIVE CRIMINAL LAW PROVISIONS COVERED

The UNCC includes a number of criminalisation obligations for the States Parties. In particular, it defines **eleven criminal offences** that Parties are required to criminalise in their national laws.

The list of offences includes cyber-dependent offences (e.g. illegal access to an information and communications technology (ICT) system) that can only be committed through use of an ICT system, as well as cyber-enabled offences (e.g. money laundering) that can be committed by other means, but the UNCC obliges criminalisation when ICT system is used.

The UNCC defines the ICT system as any device or group of interconnected or related devices, one or more of which, pursuant to a program,

gathers, stores and performs automatic processing of electronic data (Article 2(a)). The use of this term throughout the Convention is considered to be more inclusive and in line with technological advancements compared to terminology "computer" and "computer systems" adopted in the Budapest Convention.

Each State Party must criminalise the following offences:

- Illegal access to an ICT system (Article 7)
- Illegal interception (Article 8)
- Interference with electronic data (Article 9)
- Interference with an ICT system (Article 10)
- Misuse of devices (Article 11)
- ICT system- related forgery (Article 12)
- ICT system-related theft or fraud (Article 13)
- Offences related to online child sexual abuse or child sexual exploitation material (Article 14)
- Solicitation or grooming for the purpose of committing a sexual offence against a child (Article 15)
- Non-consensual dissemination of intimate images (Article 16)
- Laundering of proceeds of crime (Article 17)

Unlike the Budapest Convention, the crimes covered by the UNCC do not include copyright infringements, but impose a criminalisation obligation for other, more recently emerging crimes, especially those related to child sexual offences.

Similarly to the Budapest Convention, the UNCC obliges Parties to criminalise **attempt and accessory liability** (Article 19), as well as to adopt legislation establishing **liability of legal persons** (Article 18).

As regards **jurisdiction**, the UNCC requires States Parties to assume competence when the offence is committed in their territory or on board a vessel or an aircraft belonging to the Party (Article 22). Like the Budapest Convention, the UNCC also provides for active personality jurisdiction (where an offence is conducted by one of its nationals). The UNCC goes a step further by allowing States Parties to establish jurisdiction when the offence is committed against a national of that State Party (passive personality jurisdiction) or against the State Party.

D- SCOPE OF THE PROCEDURAL MEASURES

UNCC requires that States Parties put in place a number of procedural measures and powers for the purpose of specific criminal investigations and proceedings.

The procedural powers covered by the UNCC must be made available by Parties not only for **cybercrime**, but **any criminal offence involving evidence in electronic form**. This means that the UNCC provisions relating to procedural measures apply either where a crime is committed by use of an ICT system, or where a crime not committed by use of an ICT system (for example a murder) involves the collection of electronic evidence.

Two exceptions apply, however:

- The measure of a **real-time interception of content data** is limited to serious offences, which has to be determined by domestic law (Article 30).
- On the basis of a reservation, Parties may limit the measure of **real-time collection of traffic data** to the same range of offences to which they apply the powers and procedures of real-time interception of content data (Article 29).

E- SCOPE OF INTERNATIONAL COOPERATION

The scope of international cooperation under the UNCC includes cooperation between States Parties for the purpose of:

- The **investigation and prosecution of, and judicial proceedings in relation to the criminalised offences**, including ancillary proceedings for asset freezing and confiscation;
- The **collecting, obtaining, preserving and sharing of electronic evidence of the criminalised offences and of any serious crime**.

Unlike the Budapest Convention and its Second Additional Protocol, which apply to electronic evidence related to any criminal offence, the UNCC limits the scope of international cooperation for the purposes of collecting, obtaining, preserving and sharing of electronic evidence to serious crimes only. The UNCC defines serious crimes as offences punishable by a maximum deprivation of liberty of at least four years or a more serious penalty (Article 2(h)).

F- ENTITIES COVERED

Article 2 of the UNCC defines **service providers** as any public or private entity that:

- Provides to users of its service the ability to communicate by means of an ICT system; or
- Processes or stores electronic data on behalf of such a communications service or users of such a service.

The definition of service providers under the UNCC is virtually the same as the definition under the Budapest Convention, which refers to computer system and computer data in place of ICT system and electronic data respectively.

3. DEFINING THE TOOLBOX

A- PROCEDURAL MEASURES

Chapter IV of the UNCC includes a number of procedural measures for obtaining access to electronic data for the purpose of specific criminal investigations or proceedings, such as:

- **Expedited preservation of stored electronic data** (Article 25)
- **Expedited preservation and partial disclosure of traffic data** (Article 26)
- **Production orders** (Article 27)
- **Search and seizure of stored electronic data** (Article 28)
- **Real-time collection of traffic data** (Article 29)
- **Interception of content data** (Article 30)

The Second Additional Protocol to the Budapest Convention includes additional and advanced cross-border cooperation tools, including direct cooperation with providers of domain name registration services and service providers (Articles 6 and 7 of the Second Additional Protocol) which have not been made part of the UNCC.

On the other hand, the UNCC provisions go beyond the procedural powers of the Budapest Convention by empowering Parties with tools for **freezing, seizure and confiscation of the proceeds of crime** (Article 31), the **protection of witnesses** (Article 33) and **assistance to and protection of victims** (Article 34).

Considering the global reach of service providers, regardless of their location, Article 27 of the UNCC provides the legal framework for the implementation into the national law of the Parties to the UNCC of two types of **domestic measures that may have cross-border (extraterritorial[5]) effects**:

[5] The term "extraterritorial" is not used in the text of the UNCC itself. However, for the purposes of the present document, the term is to be understood to refer to a domestic order with potential cross-border effects.

- Domestic production orders for any type of data when a person (including a service provider) is in the territory of a Party, even if the data sought is stored in another jurisdiction (Article 27(a)); and
- Domestic production orders for subscriber information where a service provider is not necessarily present in the territory of a Party but is offering a service in the territory of such Party (Article 27(b)).

B- INTERNATIONAL COOPERATION

Chapter V of the UNCC is dedicated to international cooperation. It requires States to work closely together, adhering to applicable international legal frameworks as well as their own domestic laws.

The UNCC sets out a number of provisions relating to general principles of international cooperation and specific tools, including:

- General principles of international cooperation (Article 35)
- Protection of Personal Data (Article 36)
- Extradition (Article 37)
- Transfer of sentenced persons (Article 38)
- Transfer of criminal proceedings (Article 39)
- General principles and procedures relating to mutual legal assistance (Article 40)
- 24/7 network (Article 41)
- International cooperation for the purpose of expedited preservation of stored electronic data (Article 42)
- International cooperation for the purpose of expedited disclosure of preserved traffic data (Article 43)
- Mutual legal assistance in accessing stored electronic data (Article 44)
- Mutual legal assistance in the real-time collection of traffic data (Article 45)
- Mutual legal assistance in the interception of content data (Article 46)
- Law enforcement cooperation (Article 47)
- Joint investigations (Article 48)
- Mechanisms for the recovery of property through international cooperation in confiscation (Article 49)
- International cooperation for the purposes of confiscation (Article 50)
- Special cooperation (Article 51)
- Return and disposal of confiscated proceeds of crime or property (Article 52)

The UNCC's provisions on extradition and mutual legal assistance **supplement the existing international cooperation treaties** (mutual legal assistance treaties (MLATs)) between the Parties to the UNCC **or provide a separate international legal basis** in case no other binding international instruments apply (Article 40(7)). These provisions had to be more detailed in the UNCC compared to the corresponding provisions in the Budapest Convention to accommodate countries which do not have extensive networks of bilateral extradition and MLATs in place.

In terms of mutual legal assistance, the UNCC makes it clear that international cooperation via mutual legal assistance is based on the principle of cooperation to the widest extent possible. **Mutual legal assistance for the purposes of the collection of electronic evidence is available in relation to the offences criminalised under the UNCC, as well as serious crimes in general** (Article 40(1)).[6]

[6] Budapest Convention permits it for any criminal offence.

With regard to the expedited preservation and disclosure of data, Article 42 of the UNCC provides that, when criminal justice authorities from one Party need to preserve electronic data that is stored by means of an ICT system located in another Party of the UNCC, they are able to request that the competent authorities of the requested Party order the expeditious preservation of such data. However, there is a requirement to declare that a formal request for mutual assistance for the search or similar access to electronic data will follow. Upon receipt of a request under Article 42, the requested authorities must take all appropriate measures to expeditiously preserve the data.

Article 43 of the UNCC refers to previous preservation orders pursuant to Article 42 and only allows for the disclosure of a very narrow set of traffic data, namely the data required to allow the requesting authorities to understand that the sought information is stored by a service provider located in another country (not in the requested Party).

Beyond the reach of the Budapest Convention, the UNCC also includes provisions on direct cooperation between law enforcement of Parties to the UNCC (Article 47) and joint investigative teams (Article 48),[7] as well as provisions dealing with cooperation in asset freezing and confiscation.

24/7 NETWORK OF POINTS OF CONTACT

Inspired by the Budapest Convention (Article 35), Article 41 of the UNCC further provides a tool for expedited international cooperation on cybercrime and electronic evidence between the Parties to the UNCC.

This provision requires Parties to establish points of contact available 24 hours a day, 7 days a week, which shall facilitate, or, if permitted by its domestic law and practice, directly carry out a number of specific measures, namely:

- The provision of technical advice (Article 41(3)(a));
- The preservation of stored electronic data pursuant to Article 42 (Expedited preservation of stored electronic data) and Article 43 (Expedited disclosure of preserved traffic data) of the UNCC, including, as appropriate, information about the location of the service provider (Article 41(3)(b));
- The collection of evidence and the provision of legal information (Article 41(3)(c));
- The locating of suspects (Article 41(3)(d)); or
- The provision of electronic data to avert an emergency (Article 41(3)(e))[8].

ADDITIONAL RESOURCES ON SIRIUS

A comprehensive review of Article 35 of the Budapest Convention (24/7 Network) is available on the SIRIUS platform, as well as on the SIRIUS subpage on Eurojust's website.

[7] This measure is, however, included in the Second Additional Protocol, Article 12.

[8] The provision of electronic data to avert an emergency is not included among the activities of the 24/7 network under the Budapest Convention. However, the Second Additional Protocol will bring new responsibilities for the 24/7 network in order to enhance international cooperation between States, as well as cooperation with the private sector. Specifically, Article 9 of the Second Additional Protocol provides a basis for cooperation between authorities for the disclosure of stored computer data in emergency situations. It permits each Party to utilise their 24/7 points of contact established under the Budapest Convention to both send and receive immediate requests from a point of contact in another Party "seeking immediate assistance in obtaining from a service provider in the territory of that Party the expedited disclosure of specified, stored computer data" in an emergency situation, without the need to send an MLA request. Furthermore, pursuant to Article 10 of the Second Additional Protocol, Parties may seek expedited MLA in case of an emergency. Parties may also make a declaration that emergency MLA requests under Article 10 of the Second Additional Protocol may be sent, among other channels, from the 24/7 point of contact in the receiving country.

C- PREVENTIVE MEASURES

The UNCC includes a chapter on Preventive measures, encouraging States Parties to develop and implement policies and best practices aimed at **cybercrime prevention** (Article 53). It also promotes active participation of individuals and entities outside the public sector in the prevention of cybercrime.

The UNCC lists a number of possible preventive measures the States Parties can undertake, such as measures related to strengthening cooperation between the stakeholders, public awareness efforts and capacity building.

D- TECHNICAL ASSISTANCE AND INFORMATION EXCHANGE

Going beyond the scope of the Budapest Convention, the chapter Technical assistance and information exchange emphasises the **importance of capacity building efforts**, such as trainings, and other forms of assistance, **particularly for developing States Parties** (Article 54).[9]

To prevent and combat cybercrime more efficiently, the States Parties are also encouraged to exchange with each other expertise and knowledge on cybercrime and the collection of electronic evidence (Article 55).

Emphasising the importance of building global capacity to combat cybercrime and implement the UNCC, also by addressing discrepancies in the relevant infrastructure in States Parties, the UNCC encourages the Parties to undertake **concrete actions and provide financial and technical assistance, especially to developing countries** (Article 56). In support of this effort, States Parties are also invited to make **voluntary contributions** to a specific UN funding mechanism.

4. CONDITIONS AND SAFEGUARDS

Articles 23 and 24 of the UNCC set out conditions and safeguards applicable to all powers and procedures covered by the UNCC.

- **Purpose limitation**

In accordance with Article 23(1), the powers and procedures set out in the UNCC are to be established for the purpose of "specific" criminal investigations or proceedings, in particular cases concerning specific individuals. This excludes their use for, e.g., intelligence gathering purposes.

- **Protection of human rights**

Article 24(1) of the UNCC requires Parties to ensure that the powers and procedures established under the UNCC are subject to the protection of human rights under their domestic law. These include standards and minimum safeguards arising pursuant to a Party's obligations under applicable international human rights instruments.

Unlike the Budapest Convention, the UNCC does not include a reference to any specific human rights treaty (e.g. 1966 United Nations International Covenant on Civil and Political Rights).

- **Principle of proportionality**

Article 24(1) of the UNCC further requires Parties to apply the principle of proportionality. This will be done in accordance with each Party's relevant domestic law principles. For European countries, these principles will be derived from

[9] Although the capacity building efforts were not included in the Budapest Convention, the Council of Europe's Committee of Ministers established, in October 2013, the Cybercrime Programme Office (C-PROC) which assists countries worldwide in strengthening their legal systems capacity to respond to the challenges posed by cybercrime and electronic evidence.

the European Convention on Human Rights (ECHR) and related jurisprudences, meaning that the measures must be proportional to the nature and circumstances of the offence. Other Parties may apply related domestic law principles, such as limitations on overly broad production orders and reasonableness requirements for searches and seizures. Another example of the application of the proportionality principle is an explicit limitation to use interception measures related to content data for serious offences only (Article 30(1)).

- **Other conditions and safeguards**

Pursuant to Article 24(2) of the UNCC and in accordance with State Parties' domestic laws, applicable conditions and safeguards include, as appropriate, judicial or other independent review, the right to an effective remedy, grounds justifying application, and limitation of the scope and the duration thereof.

- **Public interest, sound administration of justice and rights of third parties**

In line with Article 24(3) of the UNCC, when applying the measures provided by the UNCC, States Parties shall first consider the proper administration of justice and other public interests (for example public safety, public health, the interests of victims, respect for private life). To the extent that it is consistent with these interests, consideration shall also be given to the impact of those measures on the rights, responsibilities and legitimate interests of third parties, which may include minimising disruption of consumer services, protection from liability for disclosure or facilitating disclosure or protection of proprietary interests[10].

- **Protection of personal data**

According to Article 36 of the UNCC, transfers of personal data under the Convention must comply with the domestic data protection laws and international legal obligations (e.g. General Data Protection Regulation for the EU Member States) of the transferring State Party.

The receiving State Party must likewise ensure that the received personal data are subject to effective and appropriate safeguards in their legal framework.

As regards the onward transfer of personal data to a third country or an international organisation, the UNCC requires that the transferring State Party seeks prior authorization for such transfer of the original transferring State Party (Article 36(3)).

Although the Budapest Convention does not contain a specific provision on protection of personal data, its Second Additional Protocol (Article 14) provides for a robust system for data protection.

ADDITIONAL RESOURCES ON SIRIUS

A review of the Second Additional Protocol to the Budapest Convention is available on the SIRIUS platform, as well as on the SIRIUS subpage on Eurojust's website.

5. THE WAY FORWARD

A- MECHANISM OF IMPLEMENTATION

The chapter on the Mechanism of implementation (Chapter VIII) establishes an institutional body, the **Conference of the States Parties to the Convention**.[11] It is aimed at:

[10] See, *mutatis mutandis*, Article 15(3) of the Budapest Convention and Explanatory Report, para. 148.

[11] The Cybercrime Convention Committee (T-CY), comprised of all the State Parties to the Budapest Convention, similarly aims at facilitating the effective use and implementation of the Convention, the exchange of information and consideration of any future amendments.

- Improving the capacity of and cooperation between the States Parties.
- Promoting and reviewing the UNCC's implementation (Article 57).

The first Conference of the States Parties must be convened by the UN Secretary General within one year after the entry into force of the Convention and, thereafter, meet regularly.

The Conference of the States Parties is tasked with a number of activities, including:

- Facilitating the effective use and implementation of the UNCC;
- Facilitating information exchange on legal, policy and technological developments pertaining to the offences under the scope of the UNCC and the collection of electronic evidence;
- Cooperating with relevant stakeholders in the public and private sector;
- Reviewing periodically the implementation of the UNCC by its States Parties;
- Elaborating and adopting supplementary protocols to the UNCC.

States Parties must inform the Conference of the States Parties about the legislative, administrative and other measures, programmes, plans and practices to implement the UNCC (Article 57(6)).

The UNCC also foresees the setting up of a **Secretariat** (Article 58), which is in charge of:

- Assisting the Conference of the States Parties in carrying out its activities under the UNCC;
- Assisting, when requested, States Parties in providing information to the Conference of the States Parties under the UNCC; and
- Ensuring coordination with the secretariats of relevant international and regional organisations.

B- MULTIPLE LEGAL FRAMEWORKS

The UNCC is neither the first nor the only existing international framework to address cybercrime and cross-border access to electronic evidence. For many countries, especially those that are Parties to the Budapest Convention[12], the UNCC represents an additional international legal framework to support their efforts in fighting cybercrime.

If countries decide to become Parties to the UNCC and the Budapest Convention, questions regarding the **relationship between the two legal instruments** in practice will have to be resolved, in addition to any other international instruments, agreements and arrangements in place between countries in this field. As regards the EU Member States, it is worth noting that the EU e-Evidence Regulation[13] specifically allows for application of other (existing or future) international agreements, on the gathering of electronic evidence[14], such as the UNCC.

When multiple legal frameworks could be applied in the same situation, the practitioners will have to choose which legal framework to give preference to. In order to make the best decision for their case, they will need to have the knowledge of different legal frameworks, their benefits, including best practices. The SIRIUS Project remains committed to assisting law enforcement and judicial authorities in navigating these and other complexities related to cross-border access to electronic evidence.

[12] See here, for the list of Parties to the Budapest Convention.

[13] Denmark did not take part in the adoption of the Regulation and is not subject to its application.

[14] Article 32 of the Regulation.