FROM PHYSICAL TO DIGITAL

ENABLING THE EFFECTIVE USE OF ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS



OSCE Organization for Security and Co-operation in Europe

Vienna, October 2026
© OSCE 2026

All rights reserved. The content of this publication may be freely used and copied for educational and other non-commercial purposes, provided that any such reproduction be accompanied by an acknowledgment of the OSCE as the source.

ISBN: 978-92-9271-689-9

Published by:
OSCE Secretariat
Transnational Threats Department
Strategic Police Matters Unit
Wallnerstrasse 6
1010 Vienna, Austria

Tel: +43-1 514 36 180
Fax: +43-1 514 36 105

email: info@osce.org | spmu@osce.org
www.osce.org

Disclaimer:
The contents of this publication, including the views, opinions, findings, interpretations and conclusions expressed herein, are those of the authors and contributors and do not necessarily reflect the official policy or position of the OSCE and its participating States. Although the OSCE has invested the utmost care in the development of this study, it accepts no liability for the accuracy or completeness of any information, for instructions or advice provided, or for misprints. The OSCE Secretariat may not be held responsible for any loss or harm arising from the use of information contained in this publication and is not responsible for the content of the external sources, including external websites referenced in this publication.

FROM PHYSICAL TO DIGITAL

ENABLING THE EFFECTIVE USE OF ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS

A study to support the development of criminal procedural powers for the digital age

ABBREVIATIONS

CoE	Council of Europe
EU	European Union
MLA	Mutual Legal Assistance
OSCE	Organization for Security and Co-operation in Europe
POC	Points of Contact
SP	Service Provider
UN	United Nations

TABLE OF CONTENTS

1. INTRODUCTION **8**

1.1. INTERNATIONAL LEGAL FRAMEWORK CONCERNING CYBERCRIME AND ELECTRONIC EVIDENCE 11

1.2. WHAT IS CYBERCRIME? 13

1.3. WHAT IS ELECTRONIC EVIDENCE? 15

2. PROCEDURAL MEASURES TO OBTAIN ELECTRONIC EVIDENCE **18**

2.1. PRESERVATION OF COMPUTER DATA 20

2.2. PRODUCTION OF COMPUTER DATA 23

2.3. SEARCH AND SEIZURE OF STORED COMPUTER DATA 26

2.4. REAL-TIME COLLECTION OF COMPUTER DATA 30

2.5. CONDITIONS AND SAFEGUARDS 32

2.6. DATA PROTECTION 34

3. INTERNATIONAL CO-OPERATION TO INVESTIGATE CYBERCRIME AND OBTAIN ELECTRONIC EVIDENCE **36**

3.1. INTERNATIONAL CO-OPERATION BETWEEN CRIMINAL JUSTICE AUTHORITIES 38

3.2. INTERNATIONAL CO-OPERATION WITH MULTINATIONAL SERVICE PROVIDERS 42

4. CONCLUSION **44**

ANNEX
CHECKLIST FOR THE IMPLEMENTATION OF PROCEDURAL MEASURES **46**

1. INTRODUCTION



Cybercrime is increasing rapidly across the OSCE area and beyond, with severe consequences for individuals, businesses and public institutions. In addition to offences committed for financial gain — such as fraud, use of malware and ransomware, and online extortion — attacks against governments, public authorities and critical infrastructure are rising. In parallel, the ever more ubiquitous use of digital devices in almost all areas of life means that electronic evidence is crucial to the investigation of the vast majority of crimes, as both perpetrators and victims leave digital traces that contain important information about the offence.

Tackling the threat of cybercrime and other contemporary crimes demands a comprehensive legal and policy framework that enables criminal justice authorities to effectively obtain and analyse electronic evidence for use in criminal proceedings, in line with relevant human rights standards. The inherently cross-border nature of cybercrime, with perpetrators, victims and electronic evidence spanning multiple jurisdictions, means that domestic provisions need to be complemented by frameworks enabling effective international co-operation between law enforcement authorities in different States, as well as between criminal justice authorities and the private sector.

The growing — and constantly evolving — threat of cybercrime and other crimes involving electronic evidence makes developing a comprehensive legal framework governing criminal investigations of these offences a particularly pressing and challenging task for policymakers and legislators. This paper aims to support them in this process by providing an overview of applicable international criminal justice standards and good practices related to procedural powers and international co-operation concerning cybercrime and electronic evidence.

By presenting the standards set out in the two main international legal instruments in the area — the Council of Europe's Convention on Cybercrime (Budapest Convention) and the UN Convention against Cybercrime (Hanoi Convention) — alongside examples of how they have been incorporated into domestic legislation in OSCE participating States, the paper can support national authorities in assessing their existing legal frameworks and identifying areas for potential improvement. It can also assist States intending to ratify these instruments by serving as a tool to guide efforts to harmonize national legislation with the provisions of the two conventions.

While comprehensive national legal frameworks are the foundation of an effective criminal justice response to cybercrime and other crimes involving electronic evidence, to be impactful they also require practitioners to have the knowledge and skills necessary to apply this legislation in their daily work. The OSCE stands ready to support participating States to build their capacities in this area through targeted training and assistance, in line with its mandate.

BOX 1

The OSCE's work on combating cybercrime

The OSCE has a mandate to support its participating States in strengthening their criminal justice response to cybercrime, while upholding human rights, fundamental freedoms and the rule of law. Based on OSCE Permanent Council Decision No. 1049 setting out the OSCE Strategic Framework for Police-Related Activities, the OSCE "facilitates, at the regional and national levels, capacity-building and the exchange of information and best practices in investigating cybercrime and dealing with cyber evidence [...] in conformity with human rights, fundamental freedoms and the rule of law".[1]

In addition to programmatic activities in this area by other OSCE executive structures, the OSCE Secretariat has implemented several dedicated multi-year extrabudgetary projects, including "Capacity-building for criminal justice practitioners combating cybercrime and cyber-enabled crime in South-Eastern Europe" (2017-2019), "Capacity-building on combating cybercrime in Central Asia" (2020-2024), "Innovative policy solutions to mitigate money laundering risks of virtual assets" (2022-ongoing), "E-VIDENCE: requesting electronic evidence across borders for investigating online criminal matters, including terrorism" (2023-2026),[2] and "Capacity-building on combating cyber-crime in Central Asia: Phase II" (2024-ongoing). At the national level, the OSCE Programme Office in Astana implements the project "Support the Republic of Kazakhstan in the development of effective policies to counter cybercrimes (Phase I)" (2023-ongoing).

The OSCE has also published several guidelines and reports in this area — for example, *Guidelines on Cybercrime Investigation* (2022), *Ensuring Human Rights Compliance in Cybercrime Investigations* (2023) or *Decoding Crypto Crime: A Guide for Law Enforcement* (2025).

1 Organization for Security and Co-operation in Europe (2012) *OSCE Strategic Framework for Police-Related Activities (PC.DEC/1049)*. Available at www.osce.org/pc/92559.

2 See also the follow-up project "CLEAR: Critical Thinking, Information and Media Literacy, Ethical AI, and Resilience for Preventing and Countering Violent Extremism and Radicalization that Lead to Terrorism": https://tntd.osce.org/project/662887.

1.1 INTERNATIONAL LEGAL FRAMEWORK CONCERNING CYBERCRIME AND ELECTRONIC EVIDENCE

There are two main international criminal justice instruments on cybercrime and electronic evidence, the Council of Europe's (CoE) Convention on Cybercrime, known as the Budapest Convention (ETS No. 185),[3] and the UN Convention against Cybercrime, known as the Hanoi Convention.[4]

The Budapest Convention is the only legally binding international convention currently in force. It was opened for signature in 2001, entered into force in 2004 and, as of October 2026, has 84 State Parties.[5] The Convention is open to accession by any State, whether or not it is a member of the CoE. Accession requires the agreement of the existing Parties before a State can be invited to accede.

The Budapest Convention provides minimum standards for both substantive cybercrime offences and for procedural measures for any offence involving electronic evidence (see sections 1.2 and 2). The latter include preservation and production orders, search and seizure of stored computer data, and real-time access to and interception of computer data. The convention also provides a legal basis for international co-operation among State Parties and establishes a 24/7 network that enables co-operation and information exchange between national points of contact (see section 3).

As the traditional mutual legal assistance (MLA) that underpins several of the Budapest Convention's key international co-operation provisions is often slow and not always effective, in 2017, the CoE started negotiations for an additional protocol. The Second Additional Protocol to the Budapest Convention on enhanced co-operation and disclosure of electronic evidence (CETS No. 224)[6] was opened for signature in May 2022 and will enter into force once it has been ratified by five States.[7] The protocol aims to facilitate more efficient access to and exchange of electronic evidence between State Parties, including through direct co-operation with service providers and measures to enhance MLA. Ratifying a protocol is a separate step from ratifying a convention, so not all parties to the Budapest Convention are parties to its protocols.

Efforts have also been undertaken to develop a global framework for combating cybercrime that would offer a legal basis for co-operation in criminal matters to all UN Member States. These discussions built on existing UN instruments facilitating international co-operation and MLA, such as the UN Convention against Transnational Organized Crime[8] and its protocols, the UN Convention against Corruption,[9] and the UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances,[10] as well as the various UN conventions and protocols addressing terrorism.[11] However, as these instruments have a limited scope of

---

3 Council of Europe (2001), *Convention on Cybercrime (ETS No. 185)*.
Available at www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185.

4 United Nations (2024), *United Nations Convention against Cybercrime*.
Available at www.unodc.org/unodc/en/cybercrime/convention/home.html

5 For up-to-date information, see the Council of Europe's website:
https://www.coe.int/en/web/cybercrime/the-budapest-convention [Accessed 31 July 2026].

6 Council of Europe (2022), *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224)*. Available at www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=224.

7 There is also the First Additional Protocol but its thematic focus falls outside the scope of this paper. For more, see Council of Europe (2003), *The First Additional Protocol to the Convention on the criminalisation of racist and xenophobic acts committed through computer systems (CETS No. 189)*.
Available at www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=189.

8 UN Office on Drugs and Crime (2000), *United Nations Convention against Transnational Organized Crime and the Protocols thereto*.
Available at www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html.

9 UN Office on Drugs and Crime (2003), *United Nations Convention against Corruption*.
Available at www.unodc.org/documents/brussels/UN_Convention_Against_Corruption.pdf.

10 UN Office on Drugs and Crime (1988), *United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances*.
Available at www.unodc.org/unodc/en/treaties/illicit-trafficking.html.

11 United Nations (no date), *Text and Status of the United Nations Conventions on Terrorism*.
Available at https://treaties.un.org/Pages/DB.aspx?path=DB/studies/page2_en.xml [Accessed 31 July 2026].

application, it was deemed necessary to create a specific convention on cybercrime and electronic evidence.

The new convention was negotiated between 2021 and 2024,[12] and opened for signature in October 2025. As of October 2026, the Hanoi Convention has a total of 96 signatories and 3 State Parties.[13] At least 40 UN Member States must ratify the instrument before it can enter into force.

Once in force, the Hanoi Convention and the existing Budapest Convention can operate in parallel, with States choosing to become parties to one or both instruments. The Hanoi Convention is comparable to the Budapest Convention in terms of its substantive and procedural provisions, and also offers a legal basis for international co-operation. Furthermore, the new convention establishes a similar 24/7 network for co-operation and information exchange. As such, the two instruments can play complementary roles in facilitating international co-operation.

Finally, it is useful to look at the approach taken by the EU in its so-called ”e-evidence package” on access to electronic evidence among its Member States.[14] Regulation (EU) 2023/1543, adopted in July 2023 and applicable from 18 August 2026, introduces new tools such as a European Preservation Order and European Production Order.[15] These orders allow competent authorities in one EU Member State to directly address a service provider, or its legal representative, in another EU Member State requesting to preserve or produce specific stored computer data.

---

12 For details, see www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home.

13 For up-to-date information, see the United Nations' website: https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XVIII-16&chapter=18&clang=_en.

14 European Commission, *E-evidence: cross-border access to electronic evidence*. Available at https://commission.europa.eu/law/cross-border-cases/judicial-cooperation/types-judicial-cooperation/e-evidence-cross-border-access-electronic-evidence_en [Accessed 31 July 2026].

15 European Parliament and Council of the European Union (2023), *Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings*. Available at: https://eur-lex.europa.eu/eli/reg/2023/1543/oj.

1.2 WHAT IS CYBERCRIME?

There is no universally accepted definition of cybercrime. However, cybercrime offences are widely recognized as falling into two sub-categories:

- **Cyber-dependant** offences specifically target computer data and systems, such as illegal access to a computer system, denial-of-service attacks against computer systems, or ransomware;
- **Cyber-enabled** offences are traditional crimes committed by using computer systems, such as fraud committed through the use of a computer system, dissemination of illegal content, or online extortion and violence. The use of computer systems can significantly increase the scale, reach and speed of these crimes.

Rather than defining cybercrime as a single concept, both the Budapest and Hanoi Conventions include a list of criminal offences instead.

1.2.1 CYBER-DEPENDENT CRIMES

The core cybercrimes, also known as cyber-dependent crimes, are offences that can only be committed using, and against, computer systems. Articles 2 to 6 of the Budapest Convention refer to offences against the confidentiality, integrity and availability of computer data and systems. These are:

- **Illegal access:** intentionally accessing a computer system without authorization, for example using another person's credentials to enter a restricted network;
- **Illegal interception:** intercepting non-public transmissions of computer data, for example secretly reading another person's emails over unsecured Wi-Fi;
- **Data interference:** intentionally altering, deteriorating, deleting or suppressing computer data, for example deploying malware that encrypts or deletes stored files;
- **System interference:** intentionally hindering or disrupting the functioning of a computer system, for example launching a distributed denial-of-service attack that disables a server or website;
- **Misuse of devices:** preparatory acts such as producing or distributing devices and computer programmes primarily for the purpose of committing cybercrime, such as developing password-cracking software or sharing stolen access codes.

These offences are largely mirrored in the Hanoi Convention (Articles 7 to 11). At the regional level, the EU Directive on attacks against information systems[16] also includes the same offences against confidentiality, integrity and availability of computer data and systems as Articles 2 to 6 of the Budapest Convention.

It is important to note that, while addressing the same offences, the language and terminology used by the different instruments vary. For instance, while the Budapest Convention refers to "computer systems" and "computer data", the Hanoi Convention speaks about "information and communications technology systems" and "electronic data".

1.2.2 CYBER-ENABLED CRIMES

While there is an established list of cyber-dependant offences, the scope of cyber-enabled offences is broader and less clearly delineated. In principle, they can cover any criminal offence that can be committed or facilitated through the use of a computer system, such as fraud, extortion and harassment, dissemination of illegal content, or the buying and selling of illegal goods.

Articles 7 to 10 of the Budapest Convention specify several such offences, including cyber-related forgery, cyber-related fraud, child sexual abuse material, and copyright-related offences.

---

16 European Parliament and Council (2013), *Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA*. Available at https://eur-lex.europa.eu/eli/dir/2013/40/oj/eng.

These offences — with the exception of copyright-related offences — are largely replicated in the Hanoi Convention (Articles 12 to 14), which also introduces offences related to solicitation or grooming for the purpose of committing a sexual offence against a child (Article 15), non-consensual dissemination of intimate images (Article 16) and laundering of proceeds of crime (Article 17).

The Hanoi Convention further underlines the broader approach to cyber-enabled crimes by requiring State Parties to ensure that criminal offences established in accordance with other applicable UN conventions and protocols are also considered as criminal offences when committed through the use of information and communications technologies. Article 4 refers to the UN instruments to which a State is already party, such as the UN Convention against Transnational Organized Crime and its protocols, the UN Convention against Corruption and the UN anti-terrorism conventions and protocols. Parties to these instruments therefore need to ensure that offences such as trafficking in human beings, trafficking in drugs and firearms, or terrorist offences, are also considered criminal offences when committed using computer systems.

The potentially wide scope of cyber-enabled crimes carries a risk of overly broad interpretation or more expansive application than originally intended, which can in turn impact human rights and fundamental freedoms such as the rights to privacy or freedom of expression. It is therefore important that domestic legislation defines the relevant offences with sufficient clarity and precision, and avoids broad or vague formulations.

1.3 WHAT IS ELECTRONIC EVIDENCE?

While both the Budapest Convention and the Hanoi Convention refer to computer data or electronic data, they do not set out a specific definition of electronic evidence. Nevertheless, the provisions of both instruments indicate what is meant by electronic evidence.

In general terms, Article 14 of the Budapest Convention on the scope of procedural provisions refers to the "collection of evidence in electronic form of a criminal offence". Similar explanations are set out in the Explanatory Report to the Budapest Convention[17] and the Council of Europe Cybercrime Convention Committee's Guidance Note on the scope of procedural powers and international co-operation provisions.[18] Reference to "evidence in electronic form of any criminal offence" is also included in Article 23 of the Hanoi Convention.

Despite the lack of a universally recognized definition of electronic evidence, it is generally accepted to incorporate three different categories of computer data:

- **Subscriber information:** information about the subscriber or user of a service, including the type of service used, and the user's identity and address, payment or billing information;
- **Traffic data**: computer data about communication by means of a computer system, generated by a computer system and indicating the communication's origin, destination, route, time, date, size, duration or type of underlying service;
- **Content data**: computer data relating to the content of the communication or transmission, such as text, image, audio or video.

Taking a phone service as an example, subscriber information would refer to the subscriber or owner of the phone number, traffic data would refer to the fact of the phone call, its destination, time and duration, and content data would be the contents of the communication. Regarding an email, subscriber data would be the sender's email address and IP address, traffic data would cover data about the addressee of the e-mail, data about its transmission and route, and content data would be the contents of the e-mail including any text, images or attachments.

This understanding of electronic evidence is reflected in the Budapest and Hanoi Conventions, as well as in the EU e-evidence package. For instance, the Budapest Convention defines subscriber information (Article 18(3)) and traffic data (Article 1(d)), but does not define content data, the definition of which can be found in the Explanatory Report. Article 2 of the Hanoi Convention provides definitions for all three categories of data.

The different categories of electronic evidence carry different implications for privacy and data protection rights, with subscriber information generally considered the least intrusive and content data the most sensitive. As a general principle, the more sensitive the category of data sought, the more rigorous the safeguards regime of authorization and oversight mechanisms should be (see Section 2 below).

---

17 Council of Europe (2001), *Explanatory Report to the Convention on Cybercrime (ETS No. 185).* Available at https://rm.coe.int/16800cce5b.

18 Council of Europe Cybercrime Convention Committee (2023), *T-CY Guidance Note #13: The scope of procedural powers and of international co-operation provisions of the Budapest Convention*.
Available at https://rm.coe.int/t-cy-2023-6-guidancenote-scope-of-powers-v9adopted/1680abc76a.

BOX 2

Unique features of electronic evidence

Electronic evidence shares many properties with traditional, physical forms of evidence but also possesses some unique characteristics:

- It is hidden. Unlike a weapon, a document or any other physical object, electronic data is often invisible to the untrained eye. Finding it can require specialists and special tools.
- It is highly volatile. Electronic data can be changed or erased very easily — by a user (intentionally or not), by the device simply running and overwriting old information, or by external factors such as a loss of power, or exposure to heat, humidity or magnetic fields. Electronic data stored on a cloud server can also be easily altered, deleted or moved to a server in another jurisdiction.
- It changes through ordinary use. Digital devices constantly rewrite their memory on their own in the background. Evidence thus can be altered without anyone intending it.
- It can be copied perfectly. A forensic digital copy is identical to the original. This means several experts can examine separate copies at the same time, for different purposes, without ever touching the original.

Because of these characteristics, how electronic evidence is collected and processed is as important as the evidence itself. It should be handled by trained specialists following approved procedures, since careless handling can alter the data accidentally and undermine its integrity. Since the technologies used to store electronic evidence are constantly evolving, it is also essential that the relevant procedures are kept up to date. The specialist field that deals with collecting, preserving and examining electronic evidence in a way that maintains its admissibility in court is called digital forensics.



2. PROCEDURAL MEASURES TO OBTAIN ELECTRONIC EVIDENCE



The role of electronic evidence in criminal proceedings extends far beyond cybercrime. The digital traces individuals leave behind every time they use a mobile phone, tablet, smart watch, or laptop or desktop computer could be of relevance to any criminal investigation. This includes not only the computer data created by individual users or devices, but also the vast amount of data that is processed and stored by service providers.

Having legislation in place to allow competent authorities to obtain computer data from any person, including service providers, is therefore a prerequisite of effective investigations in the digital age. This is reflected in both the Budapest and Hanoi Conventions, which set out specific procedural powers for criminal justice authorities to obtain electronic evidence relating to any criminal offence.

The main procedural measures enabling criminal justice authorities to access electronic evidence in criminal investigations can be grouped as follows:

- Preservation of computer data;
- Production of computer data;
- Search and seizure of stored computer data;
- Real-time collection, interception of computer data.

How these measures are applied depends on the category of data concerned, i.e. whether it is subscriber, traffic or content data being sought, as well as on the situational context (e.g., an emergency or high-risk situation may, exceptionally and when specified in law, justify more intrusive measures). This reflects the fact that different categories of data have different impacts on human rights, particularly privacy and data protection rights, and therefore require different types of safeguards and conditions. As a general rule, the principles of necessity and proportionality require that national authorities use the least intrusive means possible when conducting criminal investigations.

Although interference with any computer data related to a physical person impacts their privacy, there are important differences depending on the type of data concerned. Subscriber information is the least intrusive, covering data such as a person's name, contact details or billing information. Traffic data reveals much more about a person's behaviour, including their location and details of communications such as phone call records or internet traffic logs. Content data has the greatest impact on privacy, as it interferes with the secrecy of communications, and includes the contents of the computer data such as text, audio and video files. Requests to access content data are therefore subject to the strongest safeguards. Section 2.5 addresses these conditions and safeguards in more detail.

2.1 PRESERVATION OF COMPUTER DATA

The Budapest Convention (Articles 16 and 17) and the Hanoi Convention (Articles 25 and 26) both provide for preservation orders or preservation powers.

2.1.1 WHAT ARE PRESERVATION ORDERS?

The purpose of a preservation order is to quickly secure stored computer data in its original form to prevent it from being deleted, manipulated or rendered inaccessible. This gives competent authorities time to prepare production orders or take other procedural measures to access the data. For example, in a case involving online harassment, investigators may issue a preservation order requiring an email service provider to preserve relevant account data and transmission information, such as login records and IP addresses, to prevent the information from being deleted or otherwise lost while a formal request for access to the data is prepared. The volatile nature of electronic evidence means that a timely preservation order can often determine whether a criminal case can be made at all (see Box 2).

As the conventions refer to preserving stored computer data, a preservation order can be applied to all categories of data: subscriber information, traffic data and content data. This measure does not include the disclosure of computer data.

BOX 3

Example of a preservation order

Authorities are investigating an organized crime and drug trafficking case. They discover that the suspects are using webmail to communicate with each other. As this information could be relevant for the investigation, the authorities wish to obtain the contents of the webmail inbox (content data). As preparing and processing a production order for content data request takes time, the authorities send a preservation order to a service provider. Upon receipt of the preservation order, the service provider secures the data concerned.

As this is the least intrusive measure, the threshold for its use and procedures for authorization are not as strict as for a production order. This allows competent authorities to react quickly and send the preservation order to any physical or legal person, including a service provider. After the receipt of such an order, the person possessing or controlling the data must take steps to preserve it. According to both the Budapest and Hanoi Conventions, the maximum duration of a preservation order is 90 days. However, parties may provide a possibility to extend or renew this: in such cases, the competent authority would need to send an additional request to the service provider before the initial 90-day deadline expires.

In many cases, several service providers are involved in the transmission of communications. As a result, the conventions also provide for the possibility to trace the communications and allow partial disclosure of traffic data for this purpose. If several service providers are involved, then traffic data from one service provider may provide information related to the identification of another service provider to whom a preservation order could be sent.

2.1.2 PRESERVATION ORDERS IN NATIONAL LEGISLATION

Some OSCE participating States have integrated preservation orders into their national legislation in different ways. Box 4 presents an extract from the relevant legislation of Finland, which sets out a step-by-step approach to preservation orders and frames them as a limited measure to secure data against loss or alteration pending further legal steps.

BOX 4

Finland — Coercive Measures Act, Chapter 8[19]

Section 24 (entitled "Data retention order" in the official translation; in substance a data preservation order) establishes the legal basis for preservation orders through three subsections.[20] **Section 24(1)** provides that a preservation order may be issued by an official with the power of arrest. The order may be made prior to a search of equipment where there is reason to believe that data relevant to the investigation could be lost or altered. The order applies to any person holding or administering the data, other than the suspect, and requires that the data be maintained unchanged. It may also extend forward in time: data expected to arrive in the device or information system during the month following the order can also be covered. The recipient is entitled to a written certificate specifying the data subject to the order.

Section 24(2) extends the same rules to **traffic data**, including information relating to the origin, destination, routing, size, timing, duration and other technical characteristics of a message.

Importantly, **section 24(3)** sets a clear limit on these powers: a preservation order **does not grant authorities the right to access the content** of a message, transmission data, or other stored information. It only preserves the data as is. Where multiple service providers were involved in transmitting a message, authorities may obtain only the transmission data necessary to identify those providers.

Section 25 (Period of validity of a data preservation order) governs **duration**. It establishes that a preservation order is valid for **three months** and may be **renewed** when required for the investigation. The order must be rescinded as soon as it is no longer necessary.

Section 26 (Secrecy of a data preservation order) imposes a **duty of secrecy** on any person who receives a preservation order. This prevents the subject of the investigation from learning that their data has been frozen and potentially taking steps to destroy evidence held elsewhere. A breach of this obligation constitutes a **criminal offence under the Criminal Code**.

However, many countries' criminal procedural codes do not contain separate provisions on preservation orders. In such cases, law enforcement authorities can use general or generic police powers to send requests to preserve information, documents and other forms of computer data. While this can work effectively, the Council of Europe Cybercrime Convention Committee recommends that countries include specific procedural measures for preservation of computer data in their national legislation.[21]

Estonia is an example of this general powers approach. Rather than including a dedicated provision on preservation orders, Estonia's Code of Criminal Procedure gives investigators broad authority that can be adapted to serve the same purpose (see Box 5).

---

19 *Ministry of Justice, Finland, Coercive Measures Act (806/2011)*, unofficial translation. Available at www.finlex.fi/api/media/statute-foreign-language-translation/688063/mainPdf/main.pdf?timestamp=2011-07-21T21%3A00%3A00.000Z [Accessed 31 July 2026].

20 Note on terminology: the official English translation of the Finnish law uses the term "data retention order". However, in substance it is understood as a preservation order under Article 16 of the Budapest Convention, in line with the assessment of the Council of Europe Cybercrime Convention Committee. See: Cybercrime Convention Committee, Assessment report: Implementation of the preservation provisions of the Budapest Convention on Cybercrime, T-CY (2012)10 REV, adopted 25 January 2013, section 2.5, available at rm.coe.int/16802e722e [Accessed 5 October 2026].

21 Council of Europe Cybercrime Convention Committee (2015), *Assessment report: Implementation of the preservation provisions of the Budapest Convention on Cybercrime*. Available at https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e722e.

BOX 5

Estonia — Code of Criminal Procedure[22]

Under **§32** (Investigative bodies in criminal procedure), investigative bodies may act independently and may "demand **submission of any document necessary** for solving a criminal matter". Although this language refers to "documents", it is not limited to paper records; in practice, it extends to **digital information** held by companies, public authorities or individuals.

§215 (Obligation to comply with orders and demands of investigative bodies and prosecutors' offices) makes these demands **binding** throughout Estonia's territory, requiring immediate compliance from all recipients. Both investigators and prosecutors possess authority to issue these binding requests, with non-compliance subject to judicial enforcement through fines, although suspects and accused persons are exempt from such penalties. Although Estonia does not use the term "preservation order," these general powers allow law enforcement to **ask providers to keep data from being deleted or altered** while a formal production order is being prepared.

2.1.3 PRESERVATION ORDERS AND DATA RETENTION

The differences between a preservation order for stored computer data and the retention of data may often seem confusing. However, these two measures are different in purpose and scope.

A preservation order is sent for the purpose of a specific criminal investigation and concerns particular stored computer data: it is a criminal justice measure, usually set out in a State's criminal procedural code. In contrast, the purpose of data retention legislation is to establish a general obligation on electronic communications service providers operating in a given jurisdiction to store non-content data for a legally defined period. This requirement extends beyond the criminal justice sector and is usually provided by electronic communications legislation.

As such, while data retention can contribute to criminal investigations by ensuring that non-content computer data of electronic communications service providers is available for a certain minimum period of time, it is not a criminal procedural provision and cannot serve as a substitute for preservation powers. This has important practical implications for criminal investigations. For example, preservation orders can be applied to any category of stored computer data and sent to any entity, including any service provider. Data retention frameworks, however, cover only providers of electronic communication services operating in a given jurisdiction, and are limited to subscriber information and traffic data.

Nevertheless, the two instruments complement each other and countries can use both, if their domestic legal frameworks permit it and they have the necessary safeguards in place. In general, a data retention obligation enhances the chances that historical non-content computer data remain available and reduces the need for preservation orders for certain types of service providers at the domestic level.[23]

---

22 See the *Code of Criminal Procedure (Estonia)*, English translation published 27 January 2016; Available at www.riigiteataja.ee/en/eli/527012016001/consolide [Accessed 31 July 2026].

23 Council of Europe Cybercrime Convention Committee (2015), *Assessment report: Implementation of the preservation provisions of the Budapest Convention on Cybercrime*. Available at https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e722e.

2.2 PRODUCTION OF COMPUTER DATA

Both the Budapest Convention (Article 18) and the Hanoi Convention (Article 27) provide for production orders.

2.2.1 WHAT ARE PRODUCTION ORDERS?

While preservation orders aim to **secure** computer data in order to prevent its loss or modification, production orders are intended to enable the **disclosure** of stored computer data. A production order may follow an earlier preservation order, but can also be issued independently, without a prior preservation order for the computer data concerned.

BOX 6

Example of a production order

A law enforcement authority is investigating an alleged online child exploitation case. During the investigation, it finds that the suspect has been using an account on a social network platform, and that the service provider is located within the authority's jurisdiction. The law enforcement authority issues a production order to the service provider to obtain subscriber information and traffic data associated with the suspect's account. In this case, the production order is limited to subscriber and traffic data because the content data is already publicly accessible on the platform.

Production orders can be issued for all categories of computer data: subscriber information, traffic data and content data. This means that they can have different implications for privacy rights, with requests for more sensitive data requiring stronger conditions and safeguards. For instance, a production order for subscriber information may be issued by a responsible investigative or law enforcement authority, whereas requests for traffic or content data may require validation by a prosecutor, or an order from a prosecutor or a court.

2.2.2 PRODUCTION ORDERS TO SERVICE PROVIDERS LOCATED ABROAD

Although a production order as provided by both the Budapest and Hanoi Conventions is a domestic procedural measure, it can have an extraterritorial effect if specific conditions are met. Both conventions allow for the possibility to send a production order for subscriber information directly to a service provider offering services in the territory of the requesting party, but which is located in the territory of another party. This is particularly important given the global nature of cyberspace.

The practice of law enforcement authorities sending direct requests to a service provider located abroad is quite common. As reflected in the numerous transparency reports provided by leading international service providers,[24] this direct co-operation concerns in particular service providers based in the United States, which may voluntarily disclose data in accordance with United States legislation.

Nevertheless, challenges remain. Data disclosure depends on the internal policies and practices of a particular service provider, with a lack of effective enforcement mechanisms to compel companies to provide the data requested. When the service provider chooses not to respond and/or not to disclose data, other formal channels of international co-operation, such as MLA, need to be used. Additionally, domestic legislation in many countries prohibits such direct disclosures to foreign law enforcement authorities.

It is important to emphasize that direct co-operation should not be used as a shortcut to circumvent domestic safeguards. Even when a service provider is legally permitted to disclose data voluntarily,

---

24 For example, Google (https://transparencyreport.google.com), Meta (https://transparency.meta.com/reports/government-data-requests/), Microsoft (www.microsoft.com/en-my/digitalsafety/transparency-reports), Apple (www.apple.com/legal/transparency/).

requesting authorities should still comply with the applicable domestic authorization requirements, data protection rules and the procedural rights of the persons concerned. Direct co-operation is best understood as a complementary tool to use in appropriate cases, rather than a way to bypass the more rigorous conditions and safeguards that would otherwise apply under formal co-operation channels.

The application of Article 18 of the Budapest Convention has been discussed in detail by the Council of Europe Cybercrime Convention Committee, which has adopted a Guidance Note[25] on this topic to provide more clarity to parties to the Convention. Once the Second Additional Protocol to the Budapest Convention enters into force, it will provide further possibilities for parties to co-operate directly with service providers.

2.2.3 PRODUCTION ORDERS IN NATIONAL LEGISLATION

Countries have incorporated production orders into their national legislation in different ways. Box 7 sets out the Portuguese approach, which incorporates the possibility for production orders in the country's cybercrime law. It specifies that the order must come from a judicial authority (Article 14(1)) and includes some exceptions for data that cannot be subject to production orders, such as that from a computer system used within the legal profession, medicine, banking or journalism (Article 14(6)). It also includes a specific provision for production of subscriber data (Article 14(4)).

BOX 7

Portugal — Cybercrime Law (Law No. 109/2009)[26]

Article 14 (Injunction for providing data or granting access to data) allows a **judicial authority** to order a person or service provider to **hand over specific stored data** or to **grant access** to a computer system when this is necessary to gather evidence. The order must identify the data required, and the person or entity holding the data must provide it or grant access to the system where it is stored. Failure to comply with such an order may result in **penalties for disobedience** (Article 14(3)).

Article 14(4) also includes a dedicated rule for **subscriber information**. Service providers may be required to disclose details such as the type of communication service used, duration of the service, subscriber's identity and contact details, billing and payment information, or information about the location of communication equipment. These requests **do not extend to traffic or content data**.

At the same time, Article 14 contains **safeguards** designed to protect individual rights and professional confidentiality. First, the order cannot be directed to the **suspect** or **defendant** in the case (Article 14(5)) — the person under investigation cannot be compelled to produce data that could incriminate them. Second, production orders cannot be used to obtain data from computer systems used in certain **protected professions**: legal practice, medicine, banking and journalism (Article 14(6)). These exclusions reflect the principle that some professional relationships depend on **confidentiality** (professional privilege), and compelling disclosure would undermine them. Third, Article 14(7) clarifies that the existing rules **on professional secrecy** and **State secrets** under Portugal's Code of Criminal Procedure continue to apply, ensuring that the cybercrime law does not inadvertently override broader confidentiality protections.

Other countries include production orders within their criminal procedural codes. The Romanian example in Box 8 again highlights the different approach towards content data, given the greater interference with privacy rights entailed by giving access to the content of communications (Article 170(2)(b)).

---

25 Council of Europe Cybercrime Convention Committee (2017), *T-CY Guidance Note #10: Production orders for subscriber information (Article 18 Budapest Convention), T-CY(2015)16*. Available at https://rm.coe.int/16806f943e.

26 See extracts of Cybercrime Law No. 109/2009 of 15 September 2009 in Council of Europe (2020), *Portugal: Cybercrime Legislation*. Available at https://rm.coe.int/octocom-legal-profile-portugal/16809e5785 [Accessed 31 July 2026].

BOX 8

Romania — Criminal Procedure Code[27]

Article 170 (Surrender of objects, documents or computer data) establishes a clear legal basis for requiring individuals and entities to provide objects, documents or computer data needed in a criminal investigation. When investigators or courts have reasonable suspicion of an offence and believe that specific data may serve as evidence, they may order the person or organization holding that data to surrender it. This authority applies broadly to both natural and legal persons within Romania.

Article 170(2)(b) allows authorities to compel service providers to disclose subscriber-, user- and service-related data, but **excludes the content of communications** and other categories of data subject to a higher threshold. This reflects the broader principle that access to content data is considered **more intrusive from a privacy and fundamental rights perspective**, and therefore usually requires stricter safeguards or separate legal authority.

Article 170(2^1) to (2^5) introduces technical safeguards relating to the transmission and certification of the requested data; this is the digital equivalent of a sealed evidence bag with documented chain of custody.

27 European Commission for Democracy through Law (Venice Commission) (2018), *Romania: Law on the Criminal Procedure Code as of 7 February 2014*. Available at https://www.coe.int/en/web/venice-commission/-/cdl-ref-2018-043-e [Accessed 31 July 2026].

2.3 SEARCH AND SEIZURE OF STORED COMPUTER DATA

The Budapest Convention (Article 19) and the Hanoi Convention (Article 28) both provide for search and seizure of stored computer data.

2.3.1 WHAT IS SEARCH AND SEIZURE OF ELECTRONIC EVIDENCE?

The purpose of search and seizure provisions is to enable relevant criminal justice authorities to search or similarly access a computer system or a computer data storage medium, or a part of it, and the data stored within it. In practice, this covers the following actions (see also Box 9):

- Seizing or securing a computer system or part of it or a computer data storage medium. This could include devices such as laptops, mobile phones or smart watches, as well as storage devices such as flash drives or external hard drives;
- Making and retaining a copy of the computer data;
- Maintaining the integrity of stored computer data;
- Rendering inaccessible or removing computer data from the accessed computer system.

BOX 9

Example of search and seizure

Law enforcement authorities are investigating a cybercrime case related to ransomware and online fraud. They have identified a company that they believe is actively involved in the crime, and is providing the suspects with server and hosting services.

Sending preservation or production orders does not seem feasible, as there is a risk that the company might destroy the relevant data. Instead, the law enforcement authorities conduct a search and seizure on the company's premises. This includes the following steps:

- Law enforcement officers use force to enter the premises and secure three laptops and two hard drives;
- Officers seize the laptops that have been turned off for later inspection and forensic analysis;
- Officers access the laptops that are still running, including accessing the connected hard drives;
- Officers make forensic copies of the data for further analysis. Forensic copies or images are needed to maintain the integrity of data and to avoid later claims about possible manipulation of the data;
- One of the laptops that is still running is also connected to an internal network and a cloud service. Access to and extended search of the connected computer systems is possible and data can be accessed from the initial computer;
- The laptop connected to the cloud service contains malware and child abuse material. After making a forensic copy of this data, it is removed from the computer systems.

As the example in Box 9 shows, an important element of comprehensive search and seizure provisions is providing a legal basis to extend the search beyond the original computer system. This means that, once law enforcement authorities have lawfully accessed a computer system such as a laptop or desktop computer, it is possible to extend the search to other computer systems accessible from the initial system, for example a network of computers in a company. A key limitation under the Budapest and Hanoi Conventions is that any computer system subject to this extended search must be located in the territory of the party conducting the search. As such, this measure does not encompass cross-border searches or access to a computer system located abroad.

In this context, a frequent question is whether data stored on the cloud can be accessed from a seized device, even if the cloud provider's servers are located abroad. Neither convention clarifies whether this data should be considered as part of the system being searched or as data located abroad. In practice, States differ in what they treat as being within their territory: some enable searches to be extended to such data if they can be accessed through a "live" computer system on their territory or if access credentials were lawfully obtained, often without knowing in which jurisdiction the cloud servers sit.[28] There are also situations — for example in Dark Web investigations — where the physical location of the cloud servers storing the data cannot be determined. In such cases, State authorities typically choose to access the data concerned, if permitted under domestic law. Where a State does not treat such access as part of an extended search, reaching data stored abroad is instead regarded as transborder access to data, which is addressed in section 3.

Conducting effective search and seizure often requires assistance and the provision of information from other persons. For this purpose, both conventions require that competent authorities be empowered to order any person who has knowledge about the functioning of the computer system, or measures applied to protect the computer data it contains, to provide the information necessary to enable criminal justice authorities to perform the actions related to search and seizure, including extended search.

To address the questions raised by countries about both the legislative measures necessary to fully implement search and seizure, and their practical application, the Council of Europe Cybercrime Convention Committee has analysed the implementation of Article 19 of the Budapest Convention and provided recommendations to parties.[29]

2.3.2 SEARCH AND SEIZURE IN NATIONAL LEGISLATION

Boxes 10 and 11 provide two examples of how State Parties to the Budapest Convention have incorporated its provisions on search and seizure into their national legislation. In both cases, judicial authority is required.

Portugal's Cybercrime Law (Law No. 109/2009) sets out a structured framework for how authorities may search computer systems and seize electronic evidence during criminal proceedings (see Box 10). Romania's Criminal Procedure Code, Articles 168 and 168¹ establishes a detailed framework for searching computer systems and seizing digital evidence (see Box 11). The regime is built around strong judicial gatekeeping: a specialized judge must authorize each search in advance, and the law prescribes exact requirements for what that authorization must contain, how the search must be conducted and how the results must be documented.

In practice, these provisions allow investigators to search for and secure digital evidence, while also providing specific measures for urgent situations and safeguards for privacy-sensitive material and communications. The procedural rules are built around a central principle: more intrusive measures require higher levels of judicial oversight, and safeguards increase as the data becomes more sensitive.

In addition to ensuring that their competent authorities have the legal basis for search and seizure, States also need to develop within law enforcement the necessary technical capacity to conduct these actions.

---

28 Council of Europe Cybercrime Convention Committee (T-CY) Cloud Evidence Group (2016), *Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY. Final report*. Available at https://rm.coe.int/16806a495e (see paragraphs 41–45);
Council of Europe Cybercrime Convention Committee (2024), *Assessing Article 19 Budapest Convention on the search and seizure of stored computer data: Assessment report*. Available at https://rm.coe.int/t-cy-2023-4-assessment-rep-v92-12-dec-2024-/1680b2e13c (see Section 5.1.3).

29 Council of Europe Cybercrime Convention Committee (2024), *Assessing Article 19 Budapest Convention on the search and seizure of stored computer data: Assessment report*. Available at https://rm.coe.int/t-cy-2023-4-assessment-rep-v92-12-dec-2024-/1680b2e13c.

BOX 10

Portugal — Cybercrime Law (Law No. 109/2009)[30]

Article 15 governs the search of computer data. Article 15(1) specifies that, where a criminal investigation requires that specific stored data be obtained from a particular computer system, the competent **judicial authority** must authorize or order the search and, where possible, oversee it directly. Any such order is valid for a maximum of 30 days, after which it lapses automatically (Article 15(2)). This strict time limit is intended to prevent open-ended access to systems.

There are two exceptions allowing criminal police to act without prior judicial authorization (Article 15(3)). The first is where the person who holds or controls the data gives **voluntary, documented consent**. The second applies in cases of **terrorism**, **violent** or **highly organized crime**, where there is reasonable evidence that a crime posing **serious risk to life or health is imminent**. Even in the second scenario, the search must be **immediately reported** to the judicial authority for validation. In all cases, police must file a formal report under the Code of Criminal Procedure.

Article 15(5) requires that if, during the course of a search, the police discover that the relevant data is stored in another system — or a different part of the same system — and that data is legally accessible from the original system, the search may be **extended** by authorization of the competent authority in accordance with paragraphs 1 and 2 of the same Article.

Once relevant data is located, Article 16 governs seizure. Where computer data or documents necessary as evidence are found during a lawful search, the judicial authority may authorize or order their seizure (Article 16(1)). Criminal police may seize data without prior judicial authority, either in the course of a search lawfully ordered under Article 15 or in emergency situations (Article 16(2)). In both situations, the seizure must be validated by the judicial authority within 72 hours (Article 16(4)). This validation requirement is a general safeguard for police-executed seizures: it applies whenever the decision on seizure is taken by the police on the ground, regardless of whether the underlying search had been authorized in advance.

Additional safeguards apply where the data contains personal or intimate information (Article 16(3)), or where it relates to legal, medical, banking or journalistic activities (Article 16(5)), or to official secrets (Article 16(5)). This shows that the law explains how seizures may be carried out in a way that is proportionate and sensitive to privacy and confidentiality interests.

Depending on what is most appropriate and proportionate, authorities may seize the storage medium itself, **make a copy** of the data, **preserve the integrity of the data** in place, or **block** or **permanently remove access** to it (Article 16(7)).

Finally, Article 17 addresses a distinct and particularly sensitive category: **email** and similar **communications records**. If such material is found during a lawful search or lawful access to a computer system, the judge may authorize or order its seizure where it appears to be of significant value for establishing the truth. By treating stored email like physical mail, the law gives digital messages the same strong privacy protections as sealed letters. The idea is that the content of private correspondence, regardless of its medium, warrants the strongest procedural safeguards.

30 Council of Europe (2020), *Portugal: Cybercrime Legislation*.
Available at https://rm.coe.int/octocom-legal-profile-portugal/16809e5785 [Accessed 31 July 2026].

BOX 11

Romania — Criminal Procedure Code[31]

Article 168 sets out the basic framework for a computer search. During the investigation stage, the search may be ordered by a **Judge for Rights and Liberties**, at the request of a prosecutor, where searching a computer system or storage medium is necessary to discover and collect evidence. The warrant issued by the judge must contain the purpose of the search, the system or storage medium to be searched and the time frame for carrying it out. The judge's decision is not subject to appeal. This part of the provision shows that Romanian law places a strong emphasis on prior judicial authorization and formal warrant procedures.

If, when the search is carried out, investigators find that the data they are looking for is stored in another system or storage medium, but can be accessed from the original one, the prosecutor may immediately order the **preservation and copying** of that data and then seek an emergency warrant. To protect the integrity of digital evidence, the law allows copies to be made of the data found. If taking the original device would seriously disrupt the activities of the person holding it, a copy may be made instead.

Article 168 also sets out **safeguards** for how the search must be conducted. The search should take place in the presence of the suspect or defendant, and must be carried out by a specialist working with the judicial authorities, an outside specialist, or, under Article 168¹, specialized police officers, in the presence of the prosecutor or criminal investigation officer. A report must be prepared describing the systems searched, the steps taken and the data found.

Two final protections address privacy and secrecy. Article 168(14) requires criminal investigation bodies to ensure that the search does not unjustifiably make public the facts or circumstances of the private life of the person subject to the search. Article 168(15) provides that any data of a secret nature identified during the search must be handled in accordance with the applicable secrecy laws. During trial, the court may also order a computer search, either **on its own initiative** or at the request of the prosecutor, the parties or the victim.

31 European Commission for Democracy through Law (Venice Commission) (2018), *Romania: Law on Criminal Procedure Code as of 7 February 2014*. Available at https://www.coe.int/en/web/venice-commission/-/cdl-ref-2018-043-e [Accessed 31 July 2026].

2.4 REAL-TIME COLLECTION OF COMPUTER DATA

The real-time collection of traffic data and interception of content data are provided by the Budapest Convention (Articles 20 and 21) and the Hanoi Convention (Articles 29 and 30). These are the most intrusive measures foreseen by both conventions.

2.4.1 WHAT IS THE REAL-TIME COLLECTION OF COMPUTER DATA?

The real-time collection of traffic data and interception of content data are similar in nature and allow competent authorities to collect or record through the application of technical means real-time data related to specific communications in their territory.

Competent authorities can also compel service providers to collect or record the data concerned, as well as to co-operate with and provide assistance to the relevant criminal justice authorities. This comes with a confidentiality requirement, which obliges service providers to keep the fact of the execution of both measures and any other related information confidential.

BOX 12

Example of real-time collection of computer data

A law enforcement authority is investigating a child abuse case and has identified a server on which relevant material is being provided and accessed. There are suspects who produce and stream videos related to child abuse, as well as suspects who are downloading the content.

The law enforcement authority obtains access to the server to collect traffic data in real time and to intercept the content data, including communication and conversations between the suspects.

The reason both conventions regulate real-time collection of traffic data and interception of content data separately is the need for appropriate safeguards. Because these measures are particularly intrusive of individuals' right to private life, many countries set out specific restrictions on their use: these can include safeguards provided by the constitution. Recognizing these sensitivities, both the Budapest and Hanoi Conventions provide for flexibility in how parties integrate real-time collection of computer data into their national legislation. For example, countries can choose to set limits on the scope of the measures or establish additional requirements concerning the criminal offence, such as allowing real-time collection of data only in case of serious offences.

Collection of traffic data is generally considered less intrusive in terms of privacy rights than the interception of content data.

2.4.2 REAL-TIME COLLECTION OF COMPUTER DATA IN NATIONAL LEGISLATION

Building on the flexibility provided by international standards, countries have integrated real-time collection of computer data into their domestic legislation in different ways.

Where countries have put limits on the use of these measures, this often takes the form of the Criminal Procedure Code or other legislative act establishing a catalogue of serious offences or requiring that the criminal offence entails a certain minimum level of sanctions. In such cases, if the criminal offence is not covered by the catalogue or the level of sanction is below the necessary threshold, the real-time collection of traffic data and/or interception of content data is not permitted.

Finland's Coercive Measures Act provides the legal basis for the real-time collection of computer data through two main powers: traffic data monitoring and telecommunications interception (see Box 13 below). It limits real-time collection powers by linking them to specific categories of offences and seriousness thresholds. It also illustrates a common legislative approach of distinguishing between traffic data

and content data, with stricter conditions applying to interception of the content of communications because of its greater impact on privacy.

BOX 13

Finland — Coercive Measures Act, Chapter 10[32]

Section 6 sets out the rules on **traffic data** monitoring. This refers to the obtaining of **identifying data** about messages **sent from or received** by a network address or device, the obtaining of **location data** or the **temporary prevention** of the use of a network address or device. In simple terms, it concerns data about the communication (metadata), not the substance of any communication. A criminal investigation authority may be issued a warrant for traffic data monitoring of a device in the possession of — or presumed to be used by — a suspect, where there are grounds to suspect that person of an offence carrying a maximum sentence of **at least four years' imprisonment**.

A lower threshold of **two years** applies where the device or network address was itself the tool used to commit the offence (for instance, a computer used to hack into a system or a phone used to send threats). A warrant may also be issued for **specific listed offences regardless of sentence**, including unauthorized access to data-processing systems, child solicitation, narcotics offences, terrorism preparation, aggravated customs offences, preparation of hostage-taking or aggravated robbery.

Section 7 allows **traffic data monitoring with the consent of the possessor** of the network address or terminal device. A suspect, victim, witness or other person may agree to the monitoring of their own device in cases of offences punishable by at least two years' imprisonment, offences involving unlawful possession of the device, certain privacy-related offences committed through the device and other offences committed with the aid of the device. If the case concerns an offence that resulted in a person's death, monitoring of a device that had been in that person's possession does not require the consent of the deceased person's legal successor.

Section 3 sets out the rules on **telecommunications interception**, which is the more intrusive power. It involves monitoring, recording or otherwise processing a message in order to determine **both its content and the related identifying data**. It is reserved for the gravest offences through an exhaustive list including genocide, crimes against Finnish sovereignty, homicide, child sexual abuse, trafficking in persons, terrorism, aggravated robbery, aggravated money laundering, sabotage and aggravated narcotics offences. For serious economic offences in a commercial context — such as aggravated bribery, tax fraud, embezzlement and abuse of public office — a double condition applies: interception is permitted only where the crime was committed both for especially large benefit and in an especially methodical manner. This measure may only be directed at messages sent from or intended for a suspect.

Section 4 covers situations where **real-time interception is no longer possible** because the communication has already taken place. Authorities may instead confiscate or copy the data from a telecommunications operator or connected device, but the same strict prerequisites as for live interception under Section 3 must be met.

In practice, these provisions work as a graduated system. For example, during an investigation into a phishing network targeting Finnish banks, investigators might start with traffic data monitoring under Section 6 to map the devices and addresses involved. If a victim consents, Section 7 allows monitoring of their device at a lower threshold. As the case builds, the prosecutor may seek full content interception under Section 3. If key messages have already been sent, Section 4 allows their recovery from the operator under the same conditions.

---

32 Ministry of Justice, Finland, Coercive Measures Act (806/2011), unofficial translation. Available at www.finlex.fi/api/media/statute-foreign-language-translation/688063/mainPdf/main.pdf?timestamp=2011-07-21T21%3A00%3A00.000Z [Accessed 31 July 2026].

2.5 CONDITIONS AND SAFEGUARDS

The potential impact on human rights and the rule of law of procedural powers for investigating cybercrime and other crimes involving electronic evidence means that they need to be accompanied by proper conditions and safeguards. The more intrusive the measure, the more safeguards need to be introduced. Conditions and safeguards are also relevant when it comes to international co-operation in criminal matters. Strong and robust safeguards help build trust between countries and facilitate information exchange and collaboration among criminal justice authorities.

The Budapest Convention (Article 15) and the Hanoi Convention (Article 6) both address conditions and safeguards, including respect for human rights, related to the implementation of procedural measures. Parties must ensure these powers are subject to conditions and safeguards under their domestic law which provide adequate protection of human rights and freedoms.

The two conventions also refer to parties' obligations under international human rights law, such as those contained in the United Nations International Covenant on Civil and Political Rights,[33] the CoE Convention for the Protection of Human Rights and Fundamental Freedoms,[34] and the Charter of Fundamental Rights of the European Union.[35] In addition, the principles of necessity and proportionality deriving from these instruments need to be respected.

While setting out the overall requirement for conditions and safeguards, the Budapest and Hanoi Conventions do not provide minimum standards or thresholds, meaning that countries need to decide how to establish and implement relevant and appropriate safeguards on the basis of their constitutional framework and criminal justice system. The different applicable international frameworks provide guidance as to what these conditions and safeguards should include, for instance judicial or other independent review and oversight, the right to an effective remedy through complaints and appeals, clear grounds justifying application, and the limitation of the scope and duration of such powers.

Furthermore, the principles of necessity and proportionality require that the more intrusive the measure, the more safeguards need to be established. Countries must decide which authorities have the right to order specific procedural measures and when judicial validation or authorization would be needed. For example, while preservation of data or access to subscriber information could in principle be ordered by law enforcement authorities, access to and interception of content data would usually require a court order.

The principles of necessity and proportionality also mean that national authorities must use the least intrusive means possible at all times when conducting investigations involving electronic evidence. This requires limiting data collection to the computer data specifically needed for the purposes of the individual criminal investigation, and assessing the most feasible and proportionate measures to obtain that particular data. For example, if the required computer data can be obtained through a production order, a search and seizure might not be justified. Similarly, if only subscriber information or traffic data is needed, it is not necessary and proportionate to order the production of content data.

---

33 United Nations (1966), *International Covenant on Civil and Political Rights*. Available at www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights.

34 Council of Europe (1950), *European Convention on Human Rights (ETS No. 5)*. Available at www.echr.coe.int/european-convention-on-human-rights.

35 European Union (2012), *Charter of Fundamental Rights of the European Union*. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A12012P%2FTXT.

In conclusion, decisions on which procedural measures to use and their scope must be decided on a case-by-case basis, taking into account the specific demands of the investigation. Careful consideration is key, as such measures should also be subject to appeal and independent oversight by a court. Questions to ask when determining which measures to use include:

- What specific data is needed and why?
- What is the legal basis for requesting the data?
- What is the least intrusive method of obtaining the data?
- Who needs to authorize the specific measure to obtain the data?

Recognizing the complexity of these issues, several organizations have provided guidance to support countries in establishing and implementing effective safeguards. For example, the OSCE developed a training guide for criminal justice practitioners on ensuring human rights compliance in cybercrime investigations,[36] while the CoE has conducted several studies on the implementation of the safeguards set out in the Budapest Convention.[37]

---

36 Organization for Security and Co-operation in Europe (2023), *OSCE Training Guide for Criminal Justice Practitioners: Ensuring Human Rights Compliance in Cybercrime Investigations*. Available at www.osce.org/files/f/documents/e/3/554901.pdf.

37 Council of Europe (2011), *Article 15 – Conditions and Safeguards under the Budapest Convention on Cybercrime*. Available at https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680303194; Council of Europe (2023), *Conditions and safeguards under Article 15 of the Convention on Cybercrime in the Eastern Partnership*. Available at: https://rm.coe.int/conditions-and-safeguards-under-article-15-of-the-convention-on-cyberc/1680ad4753.

2.6 DATA PROTECTION

Data protection is a cross-cutting consideration in the exercise of procedural powers, as every preservation, production, search, seizure or interception measure involves the processing of personal data. It is also relevant for international co-operation matters, as countries have particular obligations concerning the transfer of personal data to other jurisdictions.

Protection of personal data is ensured by a wide variety of international instruments. Article 17 of the International Covenant on Civil and Political Rights protects against arbitrary or unlawful interference with privacy and provides the baseline for more detailed instruments. At the CoE level, the modernized Convention for the Protection of Individuals with Regard to the Processing of Personal Data (Convention 108+), also open to non-Member States, is legally binding on its parties.[38] For EU Member States, the General Data Protection Regulation[39] governs personal data processing in general, while the Law Enforcement Directive governs processing for the prevention, investigation, detection or prosecution of criminal offences.[40]

Although the Budapest Convention does not explicitly require the establishment of a personal data protection framework, its preamble makes a reference to this principle. In addition, its Article 15 requires that the conditions and safeguards applicable to its procedural powers be consistent with the protection of human rights and fundamental freedoms, which, in practice, includes obligations relating to privacy and personal data.

The Second Additional Protocol to the Budapest Convention builds on these general safeguards by explicitly requiring State Parties to respect data protection rights. Article 14 of the protocol sets out a detailed set of principles and obligations — including purpose limitation, data quality, retention limits, transparency, data subject rights, security and independent oversight — which State Parties must implement as a condition for using its direct co-operation tools.[41]

Similarly, the Hanoi Convention addresses personal data protection in its Article 36, though it largely defers to national law rather than establishing uniform substantive standards. The convention also contains discretionary grounds in Article 40(21), allowing States to decline MLA requests on grounds such as sovereignty, security, public order or other essential interests, which may include situations engaging data protection or human rights concerns.

In general, core data protection principles include data minimization (collecting only what is necessary and proportionate, rather than requesting broad datasets speculatively), purpose limitation (using data only for the original investigation), limited access and audit logging (restricting who can access the data and tracking activity related to it), secure storage, storage limitation (data should not be kept for longer than necessary), and protecting the data of third parties incidentally captured in the process.

---

38 Council of Europe (2018), *Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 223).* Available at www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=108.

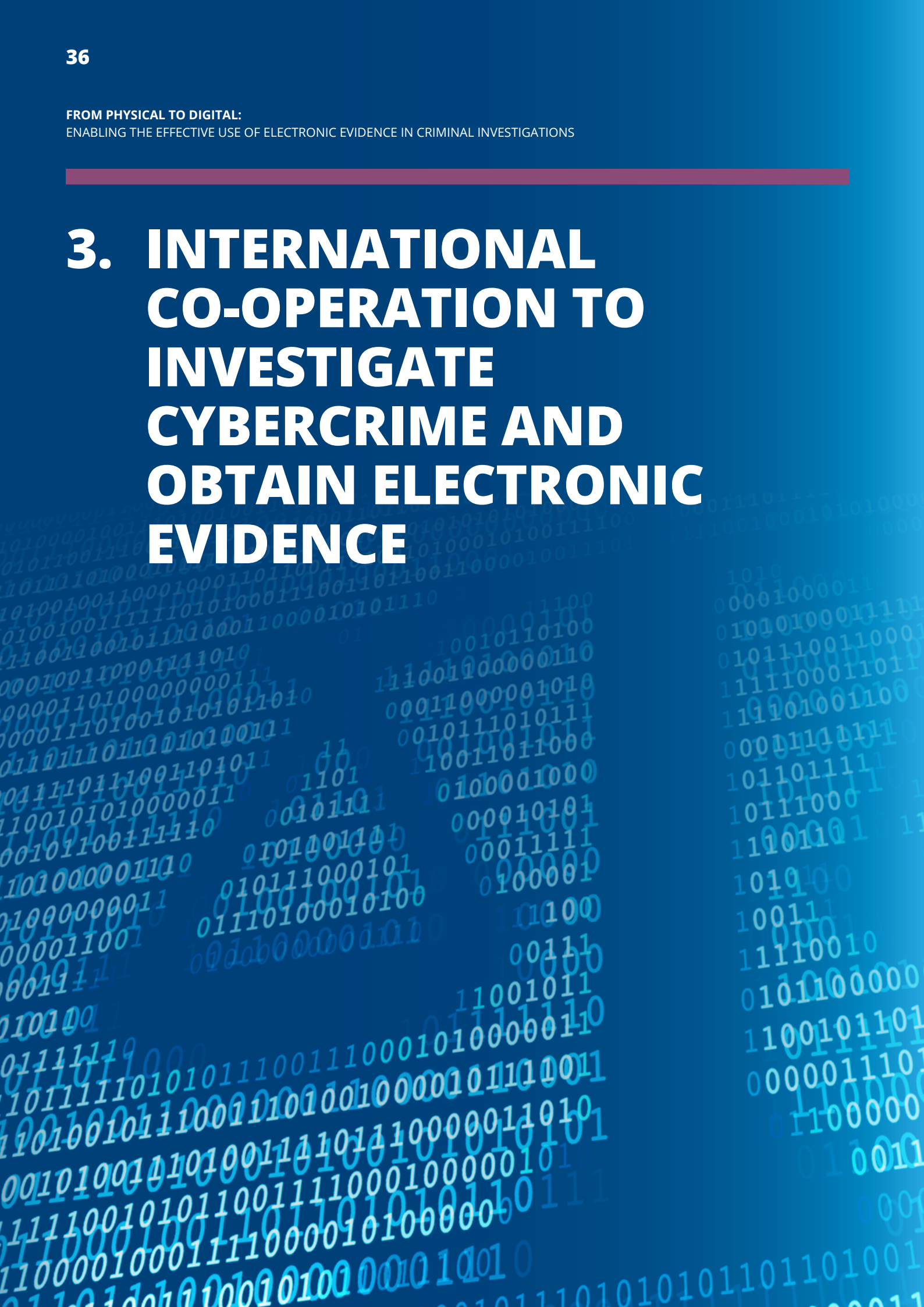
39 European Parliament and Council of European Union (2016), *Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).* Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679.

40 European Parliament and Council of European Union (2016), *Directive (EU) 2016/680 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities*. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0680.

41 Council of Europe (2022), *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224).* Available at www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=224 (see Article 14).



3. INTERNATIONAL CO-OPERATION TO INVESTIGATE CYBERCRIME AND OBTAIN ELECTRONIC EVIDENCE



Most cybercrime is transnational, with perpetrators, victims and electronic evidence often spread across jurisdictions. Even if the perpetrator and victim — of either a cybercrime or a traditional offline crime — are physically located in the same territory, critical electronic evidence could be stored abroad, giving an initially domestic investigation a cross-border element (for example, email communication stored on a server located in another State).

As a result, conducting effective criminal investigations requires countries to co-operate and exchange information. This means co-operation between criminal justice authorities in different jurisdictions. Nevertheless, as much of the electronic evidence crucial to investigations is controlled by service providers based in other countries, and stored on servers there, it also means co-operation with the private sector.

In principle, such international co-operation could take place on the basis of reciprocity. However, quick and effective co-operation is best underpinned by a clear legal basis, in the form of either bi- or multilateral treaties. Multilateral instruments help avoid the need to develop multiple individual agreements with different countries and provide a standardized framework for collaboration.

Reflecting this, provisions providing a legal basis for international co-operation between criminal justice authorities are core elements of the Budapest (Chapter III) and Hanoi Conventions (Chapter IV). In addition, the Second Additional Protocol to the Budapest Convention introduces another set of international co-operation tools, including direct co-operation with service providers, emergency procedures, joint investigation teams and accelerated MLA. Once the Hanoi Convention is in force, a State that is a party to both conventions (and their protocols) would be able to choose either one to facilitate international co-operation.

BOX 14

Challenges in international co-operation

Although international co-operation has become more crucial than ever, significant challenges remain. Law enforcement authorities can co-operate and exchange information directly but, in many cases such information is treated as police or criminal intelligence material and cannot be used as evidence in criminal proceedings. Countries therefore frequently need to rely on MLA and designated central authorities for international co-operation. As MLA procedures can be bureaucratic and time-consuming, they are not always effective or feasible, particularly given the volatile nature of electronic evidence.

For years, the CoE, the EU and other international organizations have discussed how to improve international co-operation and ensure faster access to electronic evidence stored abroad, focusing on making MLA more efficient and on developing direct co-operation with multinational service providers. The Second Additional Protocol to the Budapest Convention and the EU's e-evidence package are efforts to streamline international co-operation.

3.1 INTERNATIONAL CO-OPERATION BETWEEN CRIMINAL JUSTICE AUTHORITIES

Both the Budapest and Hanoi Conventions provide general principles and specific provisions relating to international co-operation and mutual assistance, as well as requirements for the organizational framework that parties must put in place to enable such co-operation. These complement the provisions of various other UN, CoE and EU instruments on international co-operation and information exchange by providing specific measures relevant in the context of cybercrime and electronic evidence.

3.1.1 GENERAL PRINCIPLES FOR INTERNATIONAL CO-OPERATION

The general principles relating to international co-operation and mutual assistance between criminal justice authorities in the Budapest Convention (Articles 23, 25 and 27) and the Hanoi Convention (Articles 35 and 40) are similar, and include the possibility to use the tools provided for any criminal offence within the conventions' scope. In addition, both provide grounds for refusing requests for co-operation and offer a legal basis for extradition (Budapest Convention Article 24; Hanoi Convention Article 37). For example, Article 40(22) of the Hanoi Convention requires States to refuse co-operation where there are substantial grounds to believe a request has been made for the purpose of prosecuting a person on the basis of their sex, race, religion, nationality, ethnic origin or political opinion.

However, there are some important differences. The Hanoi Convention includes international co-operation in areas such as seizure and confiscation of property, transfer of proceedings and transfer of sentenced persons, which are not included in the Budapest Convention. In contrast, the Budapest Convention can be used to obtain electronic evidence for any criminal offence, while co-operation under the Hanoi Convention is limited to offences established by the convention and serious offences that are punishable by a maximum imprisonment of at least four years (Articles 35 and 40).

3.1.2 ORGANIZATIONAL FRAMEWORK FOR INTERNATIONAL CO-OPERATION

Both conventions also set out requirements regarding the organizational framework for international co-operation: parties need to establish or designate a point of contact for the 24/7 network (Budapest Convention Article 35, Hanoi Convention Article 41) and a central authority for MLA (Budapest Convention Article 27, Hanoi Convention Article 40). These two structures correspond to the two types of co-operation provided for by both conventions: police to police co-operation between law enforcement authorities and MLA.

Under both conventions, States must specify which authority or authorities will fulfil each function when depositing the instrument of accession or ratification. While the conventions specify certain functions that must be carried out by these entities, States have some flexibility in determining where within their domestic criminal justice structures such responsibilities are best situated and what their exact tasks will be. Depending on the approach taken, police-to-police co-operation can vary. Countries which give greater powers to the 24/7 point of contact (POC) may, for instance, have more possibilities for co-operation and information exchange than others who rely more on MLA.

When it comes to the 24/7 POC, both conventions require that this entity must be available 24 hours a day, seven days a week, in order to ensure the provision of immediate assistance for the purpose of criminal investigations or proceedings under the conventions. This can include the exchange of information, expedited transmission of preservation orders, facilitation and transmission of MLA requests and other related tasks. However, parties to the Budapest Convention have adopted different approaches for fulfilling this role.[42] Some have established the 24/7 POC within the police, some in the prosecutor's office or at ministerial level, while others have designated two or more POCs (see Box 15 for examples).

---

42 Council of Europe (2025), *List of competent authorities set up in accordance with Article 27 of the Convention on Cybercrime (Budapest Convention)*. Available at https://rm.coe.int/competent-authorities-july-2025-web/1680b69201.

The 24/7 POC networks established under the conventions do not operate in isolation. In practice, they function alongside other international and regional channels for rapid communication and co-operation between criminal justice authorities, such as the INTERPOL 24/7 Contact Points network on computer-related crime[43] or, within the EU, the 24/7 on-call mechanism operated by Eurojust.[44]

The informal and expedited nature of 24/7 POC networks should not be used to bypass formal channels when evidence is intended for use in court. The 24/7 network is designed to facilitate urgent measures — such as securing preservation of data or establishing rapid contact between authorities in emergency situations — rather than as a substitute for MLA, judicial oversight or other formal requirements that ensure the admissibility and evidentiary value of the material obtained. Overly broad interpretation of police-to-police co-operation can create the risk that informal channels are used to circumvent the safeguards attached to formal co-operation mechanisms. Where evidence obtained through the 24/7 network is intended for use in criminal proceedings, formal channels should still be pursued to secure it in a manner consistent with applicable authorization and admissibility requirements.

BOX 15

Location of 24/7 POC — examples of Germany and Romania

Germany has placed its 24/7 POC for the Budapest Convention within the Federal Criminal Police Office,[45] Germany's central federal police authority, with the mandate to co-ordinate cross-border police co-operation and combat serious crime. The same unit also hosts Germany's INTERPOL and G7 24/7 POCs, which means that incoming urgent requests, whether they arrive through the Budapest Convention, INTERPOL or G7 POC networks, are received and processed by the same operational team.

Romania is an example of a State that placed its principal 24/7 POC for the Budapest Convention within the prosecution service. It sits in the Service for Combating Cybercrime under the Directorate for the Investigating Organised Crime and Terrorism within the Prosecutor's Office of the High Court of Cassation and Justice. At the same time, Romania also operates a second POC within its National Police.[46] The CoE has described this dual arrangement as efficient, because it lets each side play to its strengths: the police can use their own channels and instruments, while the prosecutor can order preservation and is competent for MLA.[47]

3.1.3 INTERNATIONAL CO-OPERATION MEASURES RELATED TO COMPUTER DATA

Complementing the general provisions, both conventions set out specific tools for international co-operation to access computer data. These measures correspond to domestic procedural powers, providing a legal basis for sending requests to another party and procedures for handling incoming requests:

- expedited preservation of stored computer data (Budapest Convention Article 29, Hanoi Convention Article 42),
- expedited disclosure of preserved traffic data (Budapest Convention Article 30, Hanoi Convention Article 43),

---

43 See INTERPOL (2021), *Position paper to the UNODC Ad Hoc Committee*. Available at www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Comments/IGOs/21COM1175-SRIUN_UseInformation_CriminalPurposes_complet.pdf.

44 See Eurojust's website: www.eurojust.europa.eu/judicial-cooperation/tasks-and-tools-eurojust/call-coordination.

45 Council of Europe (2025), *List of competent authorities set up in accordance with Article 27 of the Convention on Cybercrime (Budapest Convention)*. Available at https://rm.coe.int/competent-authorities-july-2025-web/1680b69201.

46 Ibid.

47 Council of Europe (2009), *The functioning of 24/7 points of contact for cybercrime, discussion paper, Project on Cybercrime, Economic Crime Division*, pp. 8–9. Available at https://rm.coe.int/16802fa3be.

- mutual assistance regarding accessing stored computer data (Budapest Convention Article 31, Hanoi Convention Article 44),
- real-time collection of traffic data (Budapest Convention Article 33, Hanoi Convention Article 45) and interception of content data (Budapest Convention Article 34, Hanoi Convention Article 46).

How this co-operation works in practice depends on the intrusiveness of the measure. While a preservation order can be sent within the framework of police-to-police co-operation, including by using the 24/7 network, MLA and co-operation between central authorities are required for the production as well as real-time collection and interception of data.

Because these latter measures are particularly intrusive, particularly strict conditions apply.[48] Parties must also respect the requirements of the receiving party's domestic law, including regarding dual criminality (i.e. that the offence is a crime in both jurisdictions) and sentence thresholds (i.e. that the crime merits a custodial sentence of a certain length). If such measures are not permitted in domestic investigations due to the nature of the offence or the low level of sanction, MLA is not possible.

BOX 16

Germany — incoming requests for interception under MLA[49]

The German legal framework illustrates how domestic law incorporates the principles of dual criminality and a "serious crime" threshold when giving effect to incoming MLA requests for interception of content data. It relies on two laws: the Act on International Mutual Assistance in Criminal Matters, which governs the admissibility of MLA, and the Code of Criminal Procedure, which governs the substantive conditions for interception in domestic investigations.

Under the Act on International Mutual Assistance in Criminal Matters, MLA is admissible only where the conduct underlying the foreign request would also be punishable under German law (dual criminality). For the more intrusive measures, German authorities apply the same conditions as for an equivalent domestic case. For interception of telecommunications, section 100a of the Code of Criminal Procedure sets out a catalogue of "serious crimes" for which the measure is available, including serious drug trafficking, trafficking in human beings, terrorism financing and certain serious computer-related offences.

Once in force, the Second Additional Protocol to the Budapest Convention would extend the international co-operation toolkit further. Article 8 introduces a binding mechanism for giving effect to orders issued by the competent authorities of one party for the expedited production of subscriber information and traffic data held by a service provider in another party. Article 10 establishes an emergency mutual assistance procedure, allowing a party to seek MLA from another party on a rapidly expedited basis where it considers that an emergency exists. Both provisions are designed to facilitate the most common and time-sensitive categories of cross-border request by providing a faster alternative to standard MLA procedures.[50]

3.1.4 SPONTANEOUS INFORMATION

Spontaneous information concerns a situation where a State conducting a criminal investigation discovers information that could be useful to another State, for example related to potential suspects, victims or

48 Council of Europe Cybercrime Convention Committee (2023), *T-CY Guidance Note #13 on the scope of procedural powers and international co-operation*. Available at https://rm.coe.int/t-cy-2023-6-guidancenote-scope-of-powers-v9adopted/1680abc76a .

49 *Act on International Mutual Assistance in Criminal Matters (Gesetz über die internationale Rechtshilfe in Strafsachen, IRG)*, sections 59, 66 and 67 (English translation available at https://www.gesetze-im-internet.de/englisch_irg/). See also *German Code of Criminal Procedure (StPO)*, Section 100a (English translation available at https://www.gesetze-im-internet.de/englisch_stpo/).

50 Eurojust (2024), *Article 8 of the Second Additional Protocol to the Convention on Cybercrime: Giving effect to orders from another Party for expedited production of subscriber information and traffic data*.
Available at www.eurojust.europa.eu/publication/article-8-second-additional-protocol-convention-cybercrime-giving-effect-orders-another.

property on their territory. The key difference from other international co-operation provisions is that the information can be disclosed to another party, within the limits of domestic law, without prior request.

Both conventions allow spontaneous exchange of information (Budapest Convention Article 26, Hanoi Convention Article 39), which can be transmitted through different co-operation channels, including the 24/7 network. After receiving the information, the receiving country decides how to proceed. If deemed necessary, it could send an MLA request or use another formal channel to obtain the information in a format that can be used as evidence in criminal proceedings.

This measure has proved a useful tool for information-sharing as it is flexible and does not involve the same strict rules and processes as for MLA. The Council of Europe Cybercrime Convention Committee has promoted the use of spontaneous exchange of information to build trust and facilitate co-operation, and adopted a Guidance Note to explain the measure in 2025.[51]

3.1.5 CROSS-BORDER ACCESS TO DATA

Article 32 of the Budapest Convention provides for "transborder" access to available computer data without the involvement of the competent authorities of another State. The Hanoi Convention does not include a corresponding provision.

Article 32 addresses two different situations. Under Article 32(a), a party may — without the authorization of another party — access publicly available (open source) computer data, regardless of the location of the data. This covers situations where a law enforcement officer accesses publicly available resources on the internet, such as information on a website.

The second scenario, foreseen under Article 32(b), enables a party — without the authorization of another party — to access or receive through a computer system in its territory, stored computer data located in another party, if they obtain the lawful and voluntary consent of the person who has the lawful authority to disclose the data. This covers instances where the computer data is not publicly available, for example because it is related to a password-protected website, email inbox or cloud storage service, but is disclosed to a law enforcement authority by a person with the lawful authority to do so. In such cases, the person possessing or controlling the data, and having the lawful authority to disclose it on a voluntary basis to law enforcement, can provide login credentials, passwords or access codes to that authority, or access the data and provide it to the authority. If the person does not have lawful authority to disclose data or it is not based on voluntary consent, Article 32 cannot be applied.

Several States have highlighted considerations relating to the protection of national sovereignty when applying Article 32(b). First, Article 32(b) does not include an obligation to notify the State in whose territory the data is physically stored, including in cases where the national legislation would typically require some form of authorization for access by foreign authorities. Second, the text does not expressly address the question of which law determines the "lawful authority" of the consenting person to disclose the data, and the laws of the requesting party and the State in which the data is located may diverge. Third, cloud computing environments may obscure or alter the physical location of data, while Article 32(b) is generally interpreted as applying only where the location of the data is known and situated in another party to the convention.

Against this background, the Council of Europe Cybercrime Convention Committee adopted a Guidance Note to further explain the scope and use of "transborder" access to data. [52]

---

51 Council of Europe Cybercrime Convention Committee (2025), *T-CY Guidance Note #14: Spontaneous information (Article 26 Convention on Cybercrime).* Available at https://rm.coe.int/t-cy-2025-3-en-guidancenote-art-26-v36-adopted/1680b68b7a.

52 Council of Europe Cybercrime Convention Committee (2014), *T-CY Guidance Note #3: Transborder access to data (Article 32).* Available at https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726a.

3.2 INTERNATIONAL CO-OPERATION WITH MULTINATIONAL SERVICE PROVIDERS

Reflecting the amount of potentially crucial electronic evidence held by multinational service providers (SPs) and the lengthy timeframes often required for MLAs, countries have been exploring new solutions to quickly secure and access electronic evidence. The aim is to avoid situations in which evidence is deleted, overwritten or no longer retained by the SP by the time the receiving State can execute the MLA request for its preservation or production.

As discussed in section 2.2.2, one such solution, which is already implemented by many countries, is direct co-operation with SPs. This involves providing law enforcement authorities with the necessary powers to send preservation or production orders directly to foreign SPs, in parallel to, and independently of, MLA and central authority channels. However, the lack of enforcement mechanisms under the Budapest and Hanoi Conventions means that the direct co-operation landscape is very diverse, with some SPs regularly providing requested information — at least to certain countries — and others not.

The Second Additional Protocol to the Budapest Convention looks to address these challenges by introducing a legally binding framework for international co-operation with SPs. Once it enters into force, it will introduce several new tools, including direct requests for domain name registration information, direct orders for subscriber information to a SP in another party, as well as the possibility for a competent authority to give effect to a foreign order for subscriber information and traffic data. The protocol will also enable — in narrowly defined emergency situations where there is a significant and imminent risk to the life or safety of a natural person — the possibility to disclose stored computer data, including content data, without MLA. Last but not least, it will establish emergency MLA and will require that central authorities be available on a 24/7 basis. There are no equivalent measures in the Hanoi Convention.

Until the Second Additional Protocol enters into force — and even then for countries that have not ratified it — States will need to rely on the existing provisions of the Budapest and Hanoi Conventions (once it, too enters into force) for direct requests to SPs located abroad. In the meantime, several international actors have sought to facilitate and improve direct co-operation through the development of guidelines and templates. At the UN level, the United Nations Office on Drugs and Crime published a Practical Guide for Requesting Electronic Evidence Across Borders.[53] Within the EU, the SIRIUS EU Digital Evidence Situation Reports address practical problems and concerns in order to understand why responses to requests are frequently delayed or refused, and look at possible future developments shaping cross-border access to digital evidence by law enforcement authorities.[54]

---

53 United Nations Office on Drugs and Crime (no date), *Practical Guide on Electronic Evidence*. Available at www.unodc.org/cld/en/publications/practical-guide/practical-guide.html.

54 Europol, Eurojust and European Judicial Network (2024), *SIRIUS EU Electronic Evidence Situation Report 2024*. Available at www.europol.europa.eu/publications-events/publications?q=Evidence%20Situation%20Report.

In addition, guidelines and templates have been prepared by international organizations and other relevant actors for law enforcement authorities to facilitate co-operation with SPs. These include recommendations regarding the use of POCs, templates for requests, analyses of SPs' data storage and disclosure policies, using correct channels to request information, being precise in setting out the scope and purpose of the requested information, indicating the legal basis in domestic legislation, and respecting the principles of necessity and proportionality. Major SPs such as Binance,[55] Google,[56] Meta,[57] Microsoft[58] and TikTok[59] have dedicated online portals for law enforcement to use to submit requests.

55 See www.binance.com/en/support/law-enforcement.

56 See https://lers.google.com/signup_v2/landing?hl=en.

57 See www.facebook.com/records/login/.

58 See https://v2.leportal.microsoft.com/.

59 See www.tiktok.com/legal/report/lawenforcementrequest.

4. CONCLUSION



Amid the continuous development of digital technologies, growing volume of cybercrimes and increasing importance of electronic evidence in all types of criminal investigations, ensuring that criminal procedure legislation is fit for the digital age is a priority for many States. International instruments such as the Budapest and Hanoi Conventions provide a blueprint for domestic legal frameworks for investigating and prosecuting cybercrimes and other crimes involving electronic evidence, and offer a solid legal basis for international co-operation in this area.

States can consider the following key steps when planning to introduce new procedural and international co-operation provisions related to cybercrime and electronic evidence into their domestic legal frameworks, either to bring their legislation in line with international good practice or with a view to signing and ratifying one or both of the Budapest and Hanoi Conventions.

Policies and legislation:

- Consider becoming party to international treaties enabling international co-operation on cybercrime and electronic evidence. When deciding how to proceed, consider and assess the benefits of the Budapest Convention and the Hanoi Convention.
- Review domestic legislation and ensure that it complies with international standards, including provisions on definitions, substantive law (i.e., criminal offences), procedural measures and international co-operation. Ensure offences are clearly and precisely defined to avoid overly broad interpretations that may impact human rights.
- Ensure that domestic legislation includes strong conditions and safeguards related to the collection and processing of computer data, incorporating the principles of necessity and proportionality, and effective judicial or other independent oversight.
- Develop and adopt legislation on personal data protection, including considering becoming a party to relevant international treaties. Ensure that personal data protection standards apply also to the criminal justice area.
- Ensure necessary capacity-building for criminal justice practitioners involved in obtaining electronic evidence, including on ensuring human rights compliance.

International co-operation:

- Raise awareness among, and build capacities of, authorities responsible for the MLA.
- Establish a national 24/7 POC(s) and make use of 24/7 POC networks or other networks for international co-operation, including ensuring necessary capacity-building for staff.
- Use available guidelines and other materials to facilitate and enhance the effectiveness of international co-operation, including direct co-operation with multinational SPs.
- Introduce and use templates for MLA and direct co-operation, including preservation requests and production orders.

The OSCE, with its network of field operations and long track-record of providing capacity-building support to law enforcement and criminal justice authorities on electronic evidence and cybercrime, stands ready to continue assisting participating States to ensure their criminal procedural legislation is adapted to the needs and requirements of the digital age.

ANNEX
CHECKLIST FOR THE IMPLEMENTATION OF PROCEDURAL MEASURES



This checklist can support countries in assessing whether their domestic procedural law complies with international standards. The relevant authorities can analyse each element to determine whether it is covered by domestic legislation. If not, the relevant legislative authorities should consider introducing the necessary amendments.

In this process, it is important to recognize that gaps will have a cumulative effect, impeding criminal justice processes at the national level and hindering international co-operation. For instance, if computer data cannot be used as evidence, or if domestic legislation and case law do not recognize or accept electronic evidence, procedural measures cannot be meaningfully applied. Without clear definitions of computer data and its categories, precise procedural powers, including necessary safeguards, cannot be introduced.

REQUIREMENTS	Y	N
ELECTRONIC EVIDENCE		
Computer data can be used as evidence in criminal proceedings		
Separate definition for electronic evidence		
Electronic evidence is covered by the general rules on evidence		
DEFINITIONS		
Computer system		
Computer data		
Subscriber information		
Traffic data		
Content data		
Service provider		
PROCEDURAL MEASURES: PRESERVATION ORDER		
Preservation order provided by legislation		
Preservation order as a standalone measure		
Preservation as part of general police powers		
Preservation order covers all categories of data and can be addressed to any person		
Preservation order enables partial disclosure of traffic data		

REQUIREMENTS	Y	N
PROCEDURAL MEASURES: PRODUCTION ORDER		
Production order provided by legislation		
Production order as a standalone measure		
Production order as part of general police powers		
Production order can be addressed to any person		
Production order for subscriber data — authorization provided		
Production order for traffic data — authorization provided		
Production order for content data — authorization provided		
Production order — possibility to send direct order to a Service Provider in another party		
PROCEDURAL MEASURES: SEARCH AND SEIZURE		
Search and seizure of stored computer data provided by legislation		
Search and seizure of stored computer data as a standalone measure		
Search and seizure of stored computer data as part of general search and seizure		
Extended search from an initial computer system provided		
Seizing and securing computer system or computer data storage medium		
Making and retaining copy of computer data		
Maintaining the integrity of stored computer data		
Rendering inaccessible or removing computer data in the accessed computer system		
Ordering any person to provide information and to assist search and seizure		
PROCEDURAL MEASURES: REAL-TIME COLLECTION OF TRAFFIC DATA		
Real-time collection of traffic data provided by legislation		
Real-time collection of traffic data as a standalone measure		
Real-time collection of traffic data as part of general interception of communications measure		
Ability of law enforcement authority to collect or record traffic data		
Compelling a Service Provider to collect or record or co-operate and provide assistance		

PROCEDURAL MEASURES: INTERCEPTION OF CONTENT DATA		
Interception of content data provided by legislation		
Interception of content data as a standalone measure		
Interception of content data as part of general interception of communications measure		
Ability of law enforcement authority to collect or record content data		
Compelling a Service Provider to collect or record or co-operate and provide assistance		
CONDITIONS AND SAFEGUARDS		
Conditions and safeguards are established by legislation and clearly apply to procedural measures regarding electronic evidence		
More intrusive measures are subject to additional safeguards in line with the principles of necessity and proportionality		
Data protection standards are in place and apply to the criminal justice area		



Organization for Security and
Co-operation in Europe