T-CY (2023)4
Strasbourg, 12 December 2024

Cybercrime Convention Committee (T-CY)

Assessing Article 19 Budapest Convention on the search and seizure of stored computer data: Assessment Report

Adopted by the 31st Plenary of the T-CY on 12 December 2024

Content

Abbreviations

CC	Criminal Code
CCP	Code of Criminal Procedure
CMA	Coercive Measures Act
CPC	Criminal Procedure Code
CrimPC	Swiss Criminal Procedure Code
DCCP	Dutch Code of Criminal Procedure
ECHR	European Convention on Human Rights
E.g.	For example
IPA	Investigatory Powers Act
NCIS	National Criminal Investigation Service
RIPA 2000	Regulation of Investigatory Powers Act 2000
StPO	Strafprozeßordnung (Code of Criminal Procedure)
TCA	The Cybercrime Act
TEI	Targeted Equipment Interference

1 INTRODUCTION

The Cybercrime Convention Committee (T-CY), at its 26th Plenary Session (10-11 May 2022), decided, pursuant to Article 46 of the Convention and the T-CY Rules of Procedure, to dedicate its 4th round of assessments to Article 19 of the Convention on Cybercrime on the search and seizure of stored computer data.

The purpose of the assessment is to share experience and good practices on the ways Parties have implemented this Article. Assessing Article 19 is of interest for a number of reasons, including:

- Article 19 is an important procedural power under the Convention. Sharing of information and experience on legislative and other measures as well as practices in implementing Article 19 would facilitate further reforms in current and future Parties where necessary.

- The domestic procedure of Article 19.2 – which requires each Party to adopt measures necessary to ensure that when its authorities search or access a computer system in its territory, they are able to expeditiously extend the search or similar accessing to another computer system in its territory under certain conditions – may be linked to the question of the extension of searches to other Parties' territories that remains of interest to the T-CY.

A questionnaire, adopted by the T-CY at its 27th Plenary on 29-30 November 2022, was sent to T-CY Representatives on 2 December 2022.

T-CY representatives were invited to prepare consolidated replies to this questionnaire in cooperation with their relevant domestic authorities and to submit replies in electronic form and in English or French to the T-CY Secretariat by 1 March 2023.

The T-CY Bureau presented the compilation of replies received at that point with initial comments to the 28th T-CY Plenary on 27-28 June 2023. Parties that had not contributed their replies yet, were requested to submit them by 31 August 2023.[1]

The T-CY Bureau presented a draft assessment report – based on contributions from 40 Parties that had been received by 1 August 2023 – to the 29th T-CY Plenary.

The 29th Plenary (Bucharest, 11-12 December 2023) decided to "welcome the draft assessment report on Article 19 of the Convention and the examples of implementation presented during the Plenary". It invited Parties to submit outstanding replies to the questionnaire and comments on the draft report by 31 January 2024 to permit the T-CY Secretariat and Bureau to prepare and share a complete version of the report in May 2024 for comments consideration by the 30th Plenary of the T-CY in June 2024.

The 30th Plenary (Strasbourg, 18-20 June 2024) decoded to welcome the latest version of the draft assessment report and the examples of implementation and preliminary conclusions presented during the Plenary, that contained the assessment of 58 Parties and invited:

- those Parties that have not yet submitted their replies (1 Party) or not yet responded to requests for clarification (8 Parties) to do so by 1 September 2024;

[1] https://rm.coe.int/t-cy-2023-10-plen28-rep-v3/1680abca03

- the 7 States that have become Parties since the start of this assessment cycle to participate in the present assessments and thus to submit their replies on the questionnaire by 1 September 2024;

- any Party to submit comments on the draft report, if any, by 1 September 2024;

- the T-CY Secretariat and Bureau to share a complete version of the draft assessment report with Parties by early November 2024 for comments and for consideration in view of adoption by the 31st Plenary of the T-CY in December 2024.

The final version of the report was adopted by the T-CY at its 31st Plenary.

The present report is structured as follows:

- Chapter 2 provides an overview of Article 19.

- Chapter 3 summarises the replies submitted by Parties to Part 1 of the questionnaire, that is, information on the legal basis for search and seizure.

- Chapters 4 to 8 address paragraphs 1 to 5 of Article 19 with each comprising an overview of implementation and examples of practices, followed by an assessment.

- Chapter 9 provides conclusions and recommendations as well as a summary of implementation of Article 19 by Parties.

- Chapter 10 provides appendices (1) on domestic legal provisions and (2) an overview of replies to the questionnaire.

The matrix of responses and individual analyses of Parties are summaries. T-CY members interested in details, statutory text, etc., should consult the submissions by Parties.

The examples provided in sections of this report are meant to illustrate the range of approaches taken by Parties with different legal systems and in different regions of the world when implementing Article 19. They are not necessarily intended to indicate "best practices" or "models" to adopt. These examples may direct the attention of interested Parties to other Parties from which they would like to seek more detailed information.

Replies, updates and clarifications received by 8 December 2024	
Party	**Received**
1. Albania	13 December 2023
2. Andorra	8 March 2023
3. Argentina[2]	14 April 2023
4. Armenia	31 August 2023
5. Australia	24 March 2023
6. Austria	1 March 2023
7. Azerbaijan	13 April 2024
8. Belgium	9 March 2023
9. Benin	27 September 2024
10. Bosnia and Herzegovina	27 February 2023
11. Brazil	27 March 2023/20 June 2023 (update)
12. Bulgaria	23 March 2023
13. Cabo Verde	30 January 2024
14. Cameroon	2 September 2024
15. Canada	5 September 2023
16. Chile	11 August 2023
17. Colombia[3]	27 March 2023
18. Costa Rica	23 February 2023
19. Croatia	13 March 2023
20. Cyprus	6 March 2023
21. Czech Republic	7 March 2023
22. Denmark	1 May 2023
23. Dominican Republic	3 February 2024
24. Estonia	3 May 2023
25. Fiji	10 September 2024
26. Finland	1 March 2023
27. France	22 February 2023
28. Georgia	2 March 2023
29. Germany	2 March 2023
30. Ghana	27 March 2024
31. Greece	5 September 2023
32. Grenada	19 September 2024
33. Hungary	6 March 2023
34. Iceland	20 March 2023
35. Israel	15 February 2023
36. Italy	4 September 2023
37. Japan	28 February 2023
38. Kiribati	12 September 2024
39. Latvia	20 March 2023
40. Liechtenstein	28 February 2023
41. Lithuania	24 February 2023
42. Luxembourg	1 September 2023[4]/25 September 2023 (update)
43. Malta	30 August 2023
44. Mauritius	31 October 2023
45. Monaco	27 March 2024
46. Montenegro	9 June 2023

[2] Replies from Spanish original translated to English language by a neural machine translation service.

[3] Replies from Spanish original translated to English language by a neural machine translation service.

[4] Draft version of replies.

Replies, updates and clarifications received by 8 December 2024	
Party	**Received**
47. Morocco[5]	22 May 2023
48. Netherlands	14 March 2023
49. Nigeria	27 March 2024
50. North Macedonia	23 August 2023
51. Norway	1 March 2023
52. Panama[6]	27 January 2023
53. Paraguay	28 February 2023
54. Peru	03 March 2023
55. Philippines	29 August 2023
56. Poland	16 August 2023
57. Portugal	18 April 2023
58. Republic of Moldova	30 January 2024
59. Romania	1 March 2023
60. San Marino	30 August 2024
61. Senegal	19 May 2024
62. Serbia	22 August 2023
63. Sierra Leone	12 September 2024
64. Slovak Republic	2 May 2023
65. Slovenia	28 February 2023
66. Spain	24 February 2023
67. Sri Lanka	11 December 2023
68. Sweden	20 March 2023/ 7 September (update)
69. Switzerland	17 March 2023/26 July 2023 (update)
70. Tonga	31 January 2024
71. Tunisia[7]	10 September 2024 (partial response)
72. Türkiye	03 March 2023
73. Ukraine	31 August 2023
74. United Kingdom	5 June 2024
75. United States of America	27 March 2023
Total	**74/75 received**

[5] Des amendements législatifs sont en cours concernant le Code de Procédure Pénale et ont pris leur processus de la voie législative. Ces amendements concernent plusieurs dispositions, y compris celles relatives à la cybercriminalité.

[6] Replies from Spanish original translated to English language by a neural machine translation service.

[7] Partial response received. As a result, Tunisia could not be assessed.

2 ABOUT ARTICLE 19 – SEARCH AND SEIZURE OF STORED COMPUTER DATA[8]

Most domestic criminal procedural laws include powers for the search and seizure of tangible objects in specific criminal investigations or proceedings. Many of the characteristics of general or "traditional" powers to search for and seize evidence, including related conditions and safeguards, are also applicable to computer data and systems, as noted in the Explanatory Report to the Convention.

However, there are important differences:[9]

- Computer data are intangible. General provisions covering objects or "things" may not be applicable. Domestic law should cover computer data.
- While data may be read with the use of computer systems, they cannot be seized and taken away in the same way as paper records or other objects. Domestic law should provide for a power, for example, on making copies or rendering data inaccessible.
- Due to the connectivity of computer systems, data may not be stored in the computer system that is searched, but such data may be readily accessible to that system through communication networks, such as the Internet. Additional or complementary provisions may be needed to regulate such an extension of searches.

Furthermore, the growing complexity and constant evolution of technology and devices, and of data masking techniques, such as data anonymisation or encryption, continuously raise new challenges for criminal justice authorities that need to search and seize stored computer data for the purposes of specific criminal investigations or proceedings.

The Convention's procedural powers, including Article 19, require that Parties have certain capabilities – search and seizure, for example. The evolution of technology implies that Parties must modernise their domestic procedural laws where gaps exist, to ensure that criminal justice authorities have or continue to have sufficient search and seizure powers to collect electronic evidence. Similar to other procedural law provisions of the Convention, Article 19 "ensures an equivalent or parallel capability for the obtaining or collection of computer data as exists under traditional powers and procedures for non-electronic data."[10]

For example, Article 19.2 provides the possibility to carry out a search in a computer system, in a storage medium, and also in a separate computer system which is lawfully available or accessible from the initial computer system. This latter possibility enables the searching authority to "expeditiously extend the search to another system" when, during a lawful search to a specific computer system or part of it, the searching authority forms a reasonable belief that the data sought are stored in another computer system in its territory.

Furthermore, Article 19 requires that investigators are empowered to "seize or similarly secure" accessed computer data and allows criminal justice authorities to compel any person (such as a system administrator) to assist, as is reasonable, the undertaking of the search and seizure. Given various ways to seize computer data, Article 19 provides a list of basic actions that investigators must be empowered to perform.

The search and seizure of stored computer data is an intrusive measure that can interfere with the rights of individuals. Therefore, it is essential that this measure is subject to limitations,

[8] The Explanatory Report to the Convention (paragraphs 184-204) provides additional explanations on Article 19. Available at https://rm.coe.int/16800cce5b

[9] See Paragraph 187 Explanatory Report to the Convention.

[10] Paragraph 141 Explanatory Report to the Convention.

conditions and safeguards to ensure an appropriate balance between the interests of justice and the fundamental rights of the individuals. As set forth in Article 15, the domestic law of Parties "shall provide for the adequate protection of human rights and liberties," including those rights arising pursuant to obligations each Parties has undertaken pursuant to international instruments, such as, as applicable, the International Covenant on Civil and Political Rights (ICCPR), the African Convention on Human and Peoples' Rights, the American Convention on Human Rights or the European Convention on Human Rights.

Such "… safeguards should also be adapted or developed to keep abreast of the new technological environment and new procedural powers".[11]

Thus, provisions in domestic law for the search and seizure of stored computer data in line with Article 19 that are subject to limitations, conditions and safeguards, helps Parties meet these obligations.[12]

At the same time the Convention sets out standards that ratifying states must regulate "at minimum" and thus "harmonising" in this case procedural powers. However, this does not exclude that Parties avail themselves of other powers in their national law.[13]

While Article 19 requires that Parties adopt legislation or other measures that empower authorities to take certain steps with respect to search and seizure, the Article does not specify whether that legal framework must involve the use of general "traditional" procedural powers for the search and seizure of tangible objects, powers specifically designed for the search and seizure of stored computer data, or a combination thereof.[14]

The Explanatory Report to Article 19 provides helpful guidance to Parties, as well as States interested in acceding to the Convention, as they work to structure or amend their legal framework to ensure authorities are sufficiently empowered to meet the various obligations under each paragraph of Article 19.

In short, to the extent that the elements of Article 19 cannot be fulfilled by using general or "traditional" procedural powers, Article 19 requires Parties to establish powers and procedures in addition to or complementing general or "traditional" procedural powers. Parties may thus give due consideration to establishing powers and procedures specific to stored computer data to meet these obligations. Such specific provisions could also provide greater clarity and enhance legal certainty.

---

[11] As noted in paragraph 132 of the Explanatory Report to the Convention.

[12] These obligations may include, for example, that an interference must be "in accordance with the law" (ECHR) or "laid down by law" (ICCPR), or that the "relevant legislation must specify in detail the precise circumstances in which such interferences may be permitted" (see CCPR General Comment No. 16: Article 17 (Right to Privacy) adopted at the Thirty-second Session of the Human Rights Committee, on 8 April 1988).

[13] See e.g. Explanatory report, paragraph 131.

[14] For the purposes of this report:

- "specific power" may be any statute, law, ordinance, rule, regulation with a binding force under domestic law specifically providing for search and seizure of computer data and systems;
- "general power" may be any statute, law, ordinance, rule, regulation with a binding force that does not refer to the search and seizure of computer data and systems specifically.

Article 19 – Search and seizure of stored computer data

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:

a a computer system or part of it and computer data stored therein; and
b a computer-data storage medium in which computer data may be stored in its territory.

2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.

3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:

a seize or similarly secure a computer system or part of it or a computer-data storage medium;
b make and retain a copy of those computer data;
c maintain the integrity of the relevant stored computer data;
d render inaccessible or remove those computer data in the accessed computer system.

4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.

5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

3 INFORMATION ON THE LEGAL BASIS FOR THE SEARCH AND SEIZURE (PART 1 OF THE QUESTIONNAIRE)

This section of the report summarises the replies to Part 1 of the questionnaire on the legal basis for search and seizure powers.

3.1 Legal basis: overview

More than half of the assessed Parties[15] have adopted specific powers for the search and seizure of stored computer data, that may also complement general powers.

Some Parties[16] currently largely rely only on general powers of their laws but may in some instances have practices or operating procedures to apply those for the search and seizure of stored computer data.[17]

3.2 Any type of crime

According to Article 14.2 of the Convention, the procedural powers of this treaty are not only applicable to the offences defined in Articles 2 to 11 of the Convention, but also other offences committed by means of a computer system, and the collection of electronic evidence of any offence. This approach also applies to Article 19.

Most Parties are indeed able to apply Article 19 with respect to any crime. A few Parties restrict the application of these powers based on a penalty threshold or applying the powers to a specific category of crimes regardless of the applicable threshold (e. g. crimes against computer systems, corruption offences). The most frequent cases are those in which the powers set out in a specific law apply only to a limited category of offences listed in that law.

In some Parties additional tools (such as covert access measures) are available only in cases of serious or organised crime.

3.3 Stored computer data

Article 19 applies to stored computer data. However, the Convention gives flexibility to Parties to determine themselves what situations they consider as constituting "stored computer data" or as data in "transfer" – for example, an unopened e-mail message waiting in the mailbox of an ISP until the addressee downloads it to their computer system may be considered by some Parties as stored computer data to which Art. 19 applies, whereas other Parties may treat it as data in transfer whose content could only be obtained by applying the power of interception.[18]

---

[15] Albania, Argentina, Armenia, Australia, Austria, Belgium, Bénin, Bulgaria, Cabo Verde, Cameroon, Canada, Croatia, Cyprus, Dominican Republic, Fiji, Finland, France, Georgia, Germany, Ghana, Greece, Grenada, Hungary, Israel, Italy, Japan, Kiribati, Latvia, Liechtenstein, Luxembourg, Malta, Mauritius, Monaco, Montenegro, Netherlands, Nigeria, North Macedonia, Panama, Philippines, Poland, Portugal, Romania, Senegal, Serbia, Sierra Leone, Slovak Republic, Slovenia, Spain, Sri Lanka, Sweden, Switzerland, Tonga, Türkiye, United Kingdom, USA.

[16] Andorra, Azerbaijan, Bosnia and Herzegovina, Brazil, Chile, Colombia, Costa Rica, Czech Republic, Denmark, Estonia, Iceland, Lithuania, Morocco, Norway, Peru, Paraguay, Republic of Moldova, San Marino, Ukraine.

[17] Some of these Parties reported that they are in the process of reforming their domestic laws in view of adopting specific powers for the search and seizure of stored computer data. The present assessment may support this process.

[18] Explanatory report, paragraph 190.

Most Parties indicated that they provide for a definition of computer data in a text, without specifically defining "stored". However, some Parties pointed out that stored computer data is already existing or available data at the time of the search and/or seizure, excluding future data.

Other Parties indicated that their domestic legal framework permits the seizure of evidence-relevant data stored temporarily or permanently on the provider's server (Germany, Switzerland) and that the decisive fact is that the "stored" data must not be data in transit in between two or more devices (Portugal) or data in motion (Canada), as such data can only be obtained through interception. For example, Poland and The Netherlands explicitly mentioned that an unopened e-mail or app messages are considered as stored computer data whereas the Czech Republic pointed out that it considers unopened email messages in the inbox of internet service provider as data in traffic flow that is necessary to obtain through interception and recording of the telecommunication traffic. Sweden stated that an unopened e-mail message would be considered stored computer data (accessible through a remote search), if the message has arrived at the time of or during the search.

Others distinguish between data that are stored on a computer (e.g. a downloaded e-mail attachment available offline) and computer data that are located on a computer network, for example, on the Internet, e.g. on the server of a person who operates an e-mail service available online (Latvia, Slovak Republic). Search and seizure powers apply only to the former and obtaining the latter depends on a different procedural power.

Furthermore, some Parties indicated other scenarios they encounter in practice. For example, Austria distinguished between computer data that might be obtained from the communication subscriber themselves and data that are to be collected from a service provider and is thus in the form of an actual communication. While the former can be accessed by means of search and seizure, the latter can be accessed only by means of real-time collection of computer data.

Other Parties stated that they consider cryptocurrencies to be a special type of computer data, and that measures under Article 19 may be used to seize them (see e. g. Switzerland, Liechtenstein).

One Party pointed out that its domestic legal framework does not permit them to use search and seizure in relation to content data (Panama).

There are also a few Parties whose national legislation does not contain any specific measures related to computer data, and that apply general measures.

3.4 Notification of persons concerned[19]

Although the Convention does not provide for a specific regime of notifications of persons concerned and leaves the issue to be determined by domestic law, some Parties may consider notification as an essential feature of search and seizure of stored computer data. Domestic laws of other Parties may not require such a measure.[20] The T-CY has nevertheless considered that obtaining information on notification under the national laws of the Parties to the Convention is beneficial and included such a question into the questionnaire. However, it is acknowledged that there may be situations where notification may not be appropriate, such as where, in line with domestic law, such notification may prejudice investigations.

[19] See section 8.1.1.2 for examples.

[20] Explanatory report, para. 204.

It should be noted that most Parties provide for notification of persons concerned in relation to traditional search and seizure measures. Some Parties provide for special notification provisions for search and seizure of computer data.

Numerous Parties fall into one of these categories where domestic laws require notification in some sense[21].

The original answers to the questionnaire provided by Parties illustrate the diversity and sophistication of notification requirements.

A number of Parties do not provide for any requirement of notification, especially when the search and seizure is carried out under a covert regime. However, it was emphasised that such a regime is subject to significant safeguards to ensure that any use of the measure is substantiated.

[21] Albania, Andorra, Argentina, Australia, Austria, Belgium, Bosnia and Herzegovina, Brazil, Bulgaria, Cabo Verde, Cameroon, Canada, Costa Rica, Croatia, Czech Republic, Denmark, Dominican Republic, Estonia, Finland, France, Georgia, Germany, Greece, Grenada, Iceland, Israel, Italy, Japan, Kiribati, Liechtenstein, Lithuania, Monaco, Montenegro, Netherlands, Nigeria, Norway, Panama, Paraguay, Peru, Poland, Portugal, Republic of Moldova, San Marino, Senegal, Sierra Leone, Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Türkiye, USA.

4 SEARCH OR SIMILAR ACCESSING (ASSESSMENT OF ARTICLE 19.1)

This section assesses implementation of Article 19.1:

> Article 19 – Search and seizure of stored computer data
>
> 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:
>
> a a computer system or part of it and computer data stored therein; and
> b a computer-data storage medium in which computer data may be stored in its territory.

4.1 Implementation of Article 19.1: overview

4.1.1 Legislative and other measures – summary

Parties implement Article 19.1. through various specific (computer search, computer data search, network search after the seizure, gaining remote and covert access to data) or general provisions (examples include house searches, search of premises and places or car searches) in their domestic law.

The most important condition that justifies the use of search and seizure of stored computer data indicated in the responses was court authorisation. Most of the Parties[22] require a court order[23] to authorise the search. In Austria, Belgium[24], Cabo Verde[25], Estonia, Finland, Greece,

[22] Albania, Andorra, Argentina, Armenia, Australia, Belgium, Bosnia and Herzegovina, Brazil, Bulgaria, Cabo Verde, Canada, Costa Rica, Croatia, Cyprus, Czech Republic, Denmark, Dominican Republic, Estonia, Fiji, Finland, Georgia, Germany, Hungary, Iceland, Israel, Japan, Kiribati, Latvia, Liechtenstein, Lithuania, Malta, Montenegro, Morocco, Nigeria, North Macedonia, Norway, Panama, Paraguay, Peru, Philippines, Portugal, Republic of Moldova, Romania, San Marino, Senegal, Sierra Leone, Slovak Republic, Slovenia, Spain, Tonga, Türkiye, United Kingdom and USA.

[23] Throughout the text of the report, a court order includes an order by a juge d'instruction or a similar judge. In some Parties, there may be more than one category of judge competent in decisions related to search and seizure.

[24] In Belgium an order from the prosecutor authority is necessary for a search in a computer system that has not been seized, but for which all the legal conditions for seizure have been met, while such order is not required for search in a computer system that has been seized as part of the investigation.

[25] Depending on the procedural phase in question, both the judge and the Public Prosecutor's Office can authorise or order the carrying out of a search. Furthermore, the legislature also provided for the possibility of criminal police bodies being able to carry out a search, without prior authorisation from the judicial authority, but only when: "a) It is voluntarily consented to by whoever has the availability or control of these data, as long as the consent given is, in any way, documented; b) In cases of terrorism, violent or highly organized crime, when there is well-founded evidence of the imminent commission of a crime that puts the life or integrity of any person at serious risk."

Hungary, Morocco[26], Netherlands[27], Poland, Portugal[28], Senegal, Slovak Republic, Sweden and Switzerland the search may be authorised by the prosecution authority in all or in certain cases.

States that are referred to in both groups apply different grounds in different stages of criminal proceedings. For example, an order from a prosecutor may be required in pre-trial proceedings/investigation phases, while an order from a judge may be necessary in trial/ulterior procedural phases. Other States distinguish between types of data searched or accessed and may not require court orders for searches related to subscriber information. Other grounds may apply also in relation to emergency or other urgent circumstances (see next Section).

Some examples of other procedural grounds necessary to justify application of the measure that were mentioned in responses:

- Brazil: justified reasons to believe that there is evidence of a criminal offence stored where the search will be performed.
- Canada: necessary not only to have prior judicial authorisation to search a specific place but also specifically for searching a computer in that place. Moreover, the police may seize a device but must obtain further authorisation before that device (a computer or cell phone) is searched.
- Finland: prerequisites of search stipulated by law.
- Georgia, Greece and Philippines: probable cause.
- Iceland: the main test concerns the legal requirements for search. If the data in question are kept by a third party, i.e., not in the possession of a suspect in the case, the threshold is higher than for a search that only involves suspects themselves.
- Israel: a ruling of the Supreme Court (see also practices below) included several procedural determinations concerning computer data searches.
- Japan: necessity.

[26] In the event of a preliminary investigation, a search may only be carried out with the authorisation of the competent public prosecutor and with the explicit consent of the person concerned (article 79 of the CPC), unless the offence is a terrorist offence and the person concerned refuses to give his consent, in which case the search is carried out with the written authorisation of the competent public prosecutor.

[27] The DCCP allows for executing search and seizure powers by police, and, or, a prosecutor without court authorisation. Decisive in the Dutch framework is the location where search and seizure powers are executed. E.g. when searching a car the police may operate without prior authorisation. Also, in the case of using search and seizure powers in a home, authorisation by the prosecutor may suffice. At the same time in instances (like the newly introduced article 557 DCCP on network search after the seizure of an automated work, and the often-used article 125 I DCCP on Network search) prior authorisation from the (investigative) judge is required.

[28] In Portugal, the rule is that the investigation is always directed by a prosecutor. Thus, it is a competence of the prosecutor to authorise a search. However, in ulterior phases (pre-trial or trial), a judge is also able to give the order, if necessary. This is a rare situation, as normally, by the pre-trial and trial phases, all the investigation was already made. That is, one can say that the general competence to authorise a search belongs to a prosecutor.

- Morocco: in the case of a flagrant crime, presence of the suspect or his representative or the presence of two witnesses other than the civil servants hierarchically responsible to the judicial police officer in charge of the search (Art. 60 of the CPC).

- Netherlands: order explicitly mentions the criminal acts involved, if possible, the name of the suspect and facts and circumstances justifying the execution of the power, reasonable expectation that the search will produce relevant information for the investigation at hand. The elements mentioned are shared with the police and or prosecutor that will execute the order. Most of the elements referred to are not shared with private entities, such as service providers.

- Peru: proportionality test (suitability, necessity, proportionality) and sufficiency of evidentiary elements.

- Portugal: if possible, presence of those judicial authorities that issued the order in the procedure.

- Romania: necessity in the discovery, identification and collection of evidence stored in a computer system or in a computer data storage medium.

- Senegal: searches are permissible only if the targeted data are absolutely necessary to the investigation, with strict conformance to the principle of the legality of evidence. The data must be useful for the purpose of determining the truth.

- Slovenia: reasonable grounds for suspecting that a crime was committed and the probability must be given that the electronic device contains electronic data.

- Switzerland: presumption of relevance to seizure – sufficient suspicion of the offence.

- USA: sworn statement by a law enforcement officer or attorney for the government establishing the existence of probable cause to believe the object of the search will be found within the place to be searched.

4.1.1.1 Examples of practices

- Argentina[29]: evidence other than that for which the warrant was issued

  The Code of Criminal Procedure of Argentina stipulates that if, in strict compliance with the search warrant, objects are found that provide evidence of the commission of a crime other than the one for which the warrant was issued, they shall be seized and the judge or prosecutor involved shall be informed. This is the so-called plain view digital doctrine: it admits the initiation of an investigation if evidence of a crime other than the one under investigation is found during a search, and it also extends to electronic evidence.

- Israel: conditions contained in a request for a computer search warrant

  A ruling of the Supreme Court, CrimFH 1062/21 Urich v State of Israel (11.1.2022), included several procedural determinations concerning computer data searches, including the necessary information which a request for a computer search warrant must contain: the purpose of the search, details of the computer device, details of the owner or holder of the offence and status in the investigation, and scope of

[29] Application of a similar principle was outlined in Armenia's response.

information requested in the search. The rulings in CrimFH Urich were adopted and incorporated into the Police Guideline.[30]

- Spain: prior authorisation

  Search and seizure is an investigative measure to be authorised by the courts, whether the device is located in the course of an arrest or when it is located on the occasion of a house search. Spanish legislation requires a specific authorisation in such a way that even if the court has issued a generic authorisation for the search of a particular address, it would be insufficient to examine the devices found at the time of that search, since access to the computer device or system requires express authorisation to do so.

  Therefore, if, on the occasion of a house search, the acting police force locates a device and does not have authorisation to register it, it cannot be carried out at that time but must seek prior authorisation from the judge.

- Costa Rica: procedure used

  1. Determine the probability of the existence of a crime.
  2. Identify possible hardware that may contain storage data that could be useful to the investigation (for example, mobile phones, smartwatches, computers, etc.). It doesn't have to be a specific hardware, it could be all types of hardware of a specific genre (USBs, laptops, tablets, etc.)
  3. Determine the reason, according to the specific case and evidence collected, that justifies the suspicion that potential data important to the investigation could be in the hardware identified in point 2 (for example, the access to a victim's phone in a homicide crime to determine with whom, how and when the victim interacted before the murder, or the trace of a IP address to a specific house in a child pornography case).
  4. Verify the place where the hardware usually resides (a house, workplace, outdoors, etc).
  5. Request a judge to order to seize and analyse the data contained in the hardware identified. Also, if the hardware resides in a private space, a search and entry to the private place must be requested.
  6. Execute the order.

4.1.2 Emergency or other urgent circumstances

There was a surprising degree of uniformity in Parties' approaches to urgent situations. Many Parties presume that searches require warrants, but in some situations, the usual type of warrant cannot always be obtained with the usual procedure. Parties define emergencies in different ways. However, almost all Parties have provisions in emergencies, either by a legal text or in practice, to obtain some type of warrant – perhaps prosecutorial permission – or to apply for a warrant by a special method – for example, by telephone. A number of Parties require later judicial ratification of searches conducted without prior judicial warrants. Parties' approaches are further detailed below.

Some Parties[31] provide for specific definitions of emergency/urgent circumstances in their domestic law. Examples of elements stated by Parties constituting emergency/urgent circumstances:

[30] For more details see Israel's reply to question 2.1 in the compilation of replies document

[31] Argentina, Australia, Austria, Bosnia and Herzegovina, Croatia, Czech Republic, Estonia, France, Georgia, Germany, Hungary, Iceland, Morocco, Netherlands, Norway, Spain, Switzerland, USA.

- Australia: if it is relevant to an indictable offence in or on a conveyance, necessity to exercise the power to prevent the thing from being concealed, lost or destroyed, serious and urgent circumstances.

- Austria: imminent danger - unavoidable need for immediate intervention", for example if the purpose of the investigative measure would be jeopardised by waiting for a decision by the prosecution authority.

- Bosnia and Herzegovina and Croatia: danger that the evidence will be destroyed, imminent danger for life and health, prolongation of the investigation or disabling the evidence collection or stopping the further criminal activity.

- Cabo Verde: well-founded reason to expect the imminent commission of a crime that puts the life or integrity of any person at serious risk.

- Canada: exigent circumstances – analysis whether there was an imminent danger of the loss, removal, destruction or disappearance of the evidence if the search is delayed or whether there is a degree of urgency that necessitates action by law enforcement.

- Czech Republic: risk of damage, destruction, loss of or hiding the item important for criminal proceedings.

- Estonia: immediate danger to the life, physical integrity, physical freedom or a high-value property interest of a person is involved, and where it is not possible to apply for or to issue a relevant authorisation at a proper time.

- France: the place is frequented by a person who constitutes a threat to public order.

- Georgia: where delay of action could cause loss of data relevant for investigation or may render it unavailable at a later time, or there is a realistic threat to life or limb of a person, or where an item subject of seizure has been found unexpectedly in the course of search and that object was not meant to be covered by the original search warrant.

- Germany: imminent danger - if the court order cannot be obtained without jeopardizing the purpose of the measure.

- Grenada: emergency situations as specified in the warrant (e.g. kidnapping, threat or harm to person of national security interest, or threat or harm to a child)

- Hungary: risk of delay that would significantly jeopardise the purpose of the search.

- Iceland: imminent risk that waiting for a court order could result in damage to the procedure.

- Mauritius: not defined, however, applications for warrants could explain that the circumstances are urgent.

- Morocco: terrorist offence, in cases of extreme urgency or there is a fear that evidence may be lost.

- Netherlands: reasonably expected disappearance of evidence, and when the arrival of the investigative judge cannot be awaited.

- North Macedonia: an armed or physical resistance expected; suspicion of a serious criminal offense, committed by a group, organization or a criminal enterprise; search supposed to be conducted in a public facility; a threat of possible destruction or cover up of any traces of the crime or objects important to the criminal procedure.

- Norway: danger of delay.

- Poland: urgent situation - the need to act urgently and quickly when any delay could lead to the loss, destruction or distortion of traces and evidence.

- Republic of Moldova - cases not subject to postponement or cases of flagrante delicto

- Spain: delaying the practice of the investigative measure may impair the obtaining of evidence (imminent risk that the information may disappear in whole or in part).

- Sweden: if delay entails risk - the circumstances are such that the measure would lose its purpose if not performed immediately.

- Switzerland: imminent danger that may occur or a realistic danger that the traces of the crime, the object or the assets will disappear if the search is not carried out immediately.

- United Kingdom: Urgent circumstances might include an immediate threat to life, or a credible and immediate threat to national security.[32]

- USA: imminent danger of destruction of evidence, danger to life or serious bodily injury.

Other Parties[33] rely on another source of law when handling emergencies/urgent circumstances. Although domestic laws of those Parties do not expressly provide for a definition of an emergency or urgent circumstances, they may require, for example, an imminent danger to life, integrity, health of a person, or security of a nation or a risk that evidence may be lost.

For example, Ghana stated that the CPA permits warrantless searches where an arrest is made and there is a need to conduct an immediate search or there are reasonable grounds to suspect that an item is tainted property or will provide evidence of a serious offence under the Economic and Organized Crime Act.

In Tonga, Section 123 of the Police Act could be used to conduct searches of data in emergencies, since it provides for warrantless searches in serious offence cases that meet several other elements of the section.

Some Parties also rely on verbal requests for issuing search warrants/court orders. One Party (Austria) indicated that when a competent authority for the issuance of the order can be reached by telephone, danger is not assumed to be sufficiently imminent to proceed without an order. Another Party (Montenegro) stated that a request can be made to an investigative judge by telephone, radio or by other means of electronic communication, in which case the

[32] Furthermore, The Investigation of Protected Electronic Information Revised Code of Practice August 2018 provide a non-exhaustive list of examples for exceptional urgent circumstances in which immediate compliance with a notice may be appropriate.

[33] Andorra, Belgium, Brazil, Bulgaria, Canada, Costa Rica, Cyprus, Denmark, Estonia, Finland, Israel, Japan, Lithuania, Panama, Slovenia, Türkiye.

transcript of the call shall be made and shall be certified and kept with original records. North Macedonia also relies on verbal requests. Other Parties stated that as with any urgent or emergency warrant – there is a judge on call 24/7 (Israel) or a system of 24/7 duty for judges and prosecutors (Slovak Republic).

With respect to procedural requirements to be met after a search in an emergency has begun, some Parties (Bosnia and Herzegovina, Bulgaria, Denmark, Georgia, Spain) indicated that their domestic law requires ex post facto validation by a court. If the emergency measure is not validated, the results of the investigation cannot be used as evidence.

A few Parties (Albania, Armenia, Chile, Fiji, Greece, Peru, Portugal) stated that there are no rules in place when it comes to emergency/urgent circumstances.

4.1.3 Lawfully acquired credentials

Law enforcement authorities that are conducting searches may lawfully obtain access credentials in various ways – from a collaborator, from electronic storage to which they have legitimate access, from paper notes, and so on. The assessment examined the extent to which lawfully obtained access credentials may be used in searches, including whether authorities must obtain supplementary judicial permission to use the credentials.

Competent authorities of many Parties[34] are empowered by legislation or by jurisprudence (Spain, Switzerland) to search or similarly access a computer system and data therein using lawfully acquired access credentials.

Some Parties adopted internal standard procedures and guidelines where the use of lawfully acquired credentials is regulated (e. g. Poland).

The issue is not regulated in the domestic laws of some Parties (Bosnia and Herzegovina, Cabo Verde, Hungary, Latvia, Norway, Portugal, Slovak Republic, Türkiye). Some Parties indicated that, though there is no specific provision with regard to accessing the system using access credentials, their applicable domestic law provides that the court in its decision authorises the right to access and search (e. g. Albania).

Several Parties (Austria, Bulgaria, Iceland) indicated that the authorities may use voluntarily disclosed credentials (Germany, Romania, Slovak Republic, USA), while several (Austria, Bulgaria, Iceland) also specifically indicated that their authorities firstly ask the person who presumably knows the password to disclose it voluntarily before other measures are used.

A number of Parties (Austria, Brazil, Czech Republic) emphasised that the person cannot be forced to hand over the data if such handing over could breach the person's constitutional rights, such as the right to not incriminate oneself.

Examples of practices include:

- Australia: account takeover warrants

  These allow authorities to take control of a person's online account for the purposes of gathering evidence about offences which carry a term of imprisonment of 3 years or more. An online account may include, for example, an account on a dark web

[34] Andorra, Armenia, Australia, Austria, Belgium, Brazil, Bulgaria, Canada, Costa Rica, Croatia, Cyprus, Czech Republic, Denmark, Dominican Republic, Estonia, Finland, France, Georgia, Ghana, Greece, Iceland, Israel, Japan, Liechtenstein, Montenegro, Netherlands, Nigeria, Panama, Philippines, Republic of Moldova, Romania, Senegal, Sierra Leone, Slovenia, Sweden, United Kingdom, USA.

forum or marketplace, an email service, social media account, subscription to a news service or a user profile of a messaging platform. An account takeover warrant facilitates covert and compelled (without consent of the account holder) account takeovers.

An account takeover warrant allows authorities to use account credentials to change passwords, or other log-in details, associated with an account to lock out the account holder or user to gain exclusive access to the account. Any other activities, such as accessing data or performing undercover activities while in control of the account such as assuming a false identity, must be performed under a separate warrant or authorisation. At the conclusion of the warrant, the officer must take reasonable steps to restore access to the account to the account holder, if it is lawful for the account holder to operate the account.

- Brazil: steps typically taken to execute the power of using lawfully acquired access credentials

  - The competent authorities must submit a request for the court order or search warrant to the competent court, providing the relevant facts and evidence supporting the need to access the computer system and data therein using lawfully acquired access credentials.
  - If the court grants the authorisation, the authorities will use the access credentials to access the computer system and data therein, in accordance with the terms and conditions specified in the court order or search warrant.
  - After the search or access is completed, the competent authorities must submit a report to the court, describing the results of the search or access, and providing a list of the data or information obtained.

- Germany: consent to the measure

  A search warrant pursuant to Section 105 of the Code of Criminal Procedure is dispensable if the person concerned (in the case of several joint custody holders: all of them) expressly consents to the search. Simply letting it happen without objection is not sufficient, but unambiguous, silent consent is sufficient. This consent to the search will be documented.

- Norway: proportionality requirement

  The general provisions on proportionality in the Criminal Procedure Act Section 170a apply:
  Section 170 a:
  A coercive measure may only be used when there are sufficient grounds for it. The coercive measure may not be used when it would be disproportionate to the nature of the case and the circumstances. The issue of proportionality would apply to how the access credentials are used, how this might affect third parties, the necessity of use, and the time period for access.

4.1.4 Covert remote access

The assessment also studied whether Parties may remotely access data secretly. The domestic law of several Parties[35] does not authorise their authorities to search or otherwise access a computer system and its data using covert remote access.

[35] Albania, Austria, Bosnia and Herzegovina, Brazil, Bulgaria, Costa Rica, Cyprus, Dominican Republic, Ghana, Grenada, Israel, Japan, Mauritius, Panama, Portugal, Sierra Leone, Slovak Republic.

Other Parties may do so mostly when other special circumstances are met. These may include availability of the measure only in relation to certain offences[36] and other special circumstances, such as a target's use of sophisticated technology[37] or very limited duration.[38]

Examples of specific covert remote access measures or measures alternative to covert remote access as provided by domestic laws of Parties include:

- Andorra: undercover police officer, who could, if necessary, act on a computer system (Article 122 ter of the CPC).
- Australia: delayed notification search warrant (Part IAAA of the Crimes Act), remote and covert search of electronic devices and content (Division 4 of Chapter 2 of the SD Act).
- Belgium: secret searches in a computer system (article 90ter of the Code of Criminal Procedure).
- Chile: use of computer programs that allow remote access and apprehending the content of a device, computer or computer system, without the knowledge of its user (Art. 225bis of the CPC).
- Czech Republic: surveillance of Persons and Items (158d par. 3 and 4 of the CPC).
- Denmark: secret search, data reading and interference with correspondence (Section 799 of the Administration of Justice Act).
- Estonia: covert surveillance, covert collection of samples for comparison and conduct of initial investigations, covert examination and substitution of an object § 126 of the CPC).
- Fiji: collection of real-time collection of traffic data and interception of content data (Sections 22 and 23 of the TCA).
- Finland: technical surveillance of a device (Section 23, Coercive Measures Act. Act).
- France: capturing computer data, 3 special investigative techniques: the use of IMSI-catcher, sound recording and image fixation, and the capture of computer data.
- Georgia: covert remote access to a computer system (Article 143(1)b of the CCP).
- Germany: covert remote search of information technology systems (Section 100b of the StPO).
- Hungary: secret surveillance of an information system, secret search, secret surveillance of a locality, secret interception of a consignment, interception of communications (Sections 231-234 of CCP).

[36] Andorra, Argentina (in some jurisdictions), Australia, Belgium, Cabo Verde, Czech Republic, Denmark, Estonia, France, Georgia, Germany, Hungary, Iceland, Latvia, Lithuania, Montenegro, Netherlands, Norway, Republic of Moldova, Slovenia, Spain, Sweden, Türkiye.

[37] Belgium, Croatia, Finland, France, Germany, Montenegro, Spain, Switzerland, Türkiye, USA.

[38] Chile (maximum 30 days, the guarantee judge may extend this period for periods of up to the same duration, with a maximum of 60 days).

- Iceland: telephone tapping and other comparable measures (Chapter XI. of the CCP).
- Latvia: control of Data Located in an Automated Data Processing System and Control of the Content of Transmitted Data (Articles 219 and 220 of the CPC respectively).
- Lithuania: actions of pre-trial investigators without disclosing their identities (Article 158 of the CPC).
- Luxembourg: special investigative measures (Art. 88-1 to 88-4 of the CPC).
- Montenegro: secret surveillance measures (Chapter 9 of the CPC).
- Netherlands: "gaining remote and covert access" / "legal hacking" (Article 126nba DCCP or Article 181 jo 126ng DCCP with prior judicial authorisation).
- Norway: data reading (Section 216 o and 216 p of the CPC).
- North Macedonia: secret access and search of computer systems (Article 252.4).
- Republic of Moldova: Access, interception and recording of computer data (Article 138 of the CPC)
- Romania: surveillance measure performed covertly using lawfully acquired credentials (Article 138.1.b)
- Senegal: installation and use of remote tools to obtain evidence useful for a case (Article 90-10).
- Slovenia: possibility of controlling the computer system of a bank or other legal entity that performs financial or other economic activity.
- Spain: remote searches of computer system (Article 588 septies of the CPL).
- Sweden: secret data interception (Secret Data Interception Act).
- Switzerland: using special IT programmes pursuant (Articles 269ter and 269quater CrimPC).
- Tonga: interception of electronic communications (Section 14 of the Computer Crimes Act).
- Turkey: investigation of the offense of online illegal betting (Article 5 of Law No. 7258).
- United Kingdom: Targeted Equipment Interference (TEI) warrant (s99(2) of the Investigatory Powers Act 2016).
- USA: remote access to search electronic storage media (Federal Rule of Criminal Procedure 41(b)(6)).

Responses suggest that the term "covert remote access" is understood differently by various Parties. Some Parties refer explicitly to remote searches of computer systems including introducing a special software in the system, others refer to traditional surveillance powers or use of undercover agents.

Numerous Parties[39] pointed out that a court order is required to authorise such a measure. At least one Party (Greece) does not require such a court order in some cases.

Some Parties (Belgium, Denmark, Estonia, France, Georgia, Hungary, Latvia, Norway, Spain, Switzerland) also indicated that the measure includes the possibility of real time collection of data, and requirements exist with respect to notification (Australia, Belgium, Denmark, Georgia[40], Germany, Lithuania, Netherlands).

With respect to other safeguards, some Parties (Costa Rica, Denmark, Estonia, Finland, Germany, Israel, Netherlands, Norway, Spain) stated that the measure can last only for a limited duration. One Party (Armenia) indicated that, although no specific provision regulates covert remote search, such measures may be carried out in practice.

Examples of practices include:

- France: capture of computer data
  - Articles 706-102-1 and 706-102-2 of the Code of Criminal Procedure define the measure.
  - It is possible to remotely and continuously capture data (text, images, audio, etc.) on a target computer terminal (computer, telephone, tablet, etc.).
  - Using this technique, investigators can both access the data contained on a digital terminal and intercept data flows.
  - This solution has the advantage of bypassing the encryption of communications. In addition to recording keystrokes and capturing screen copies, the technical device used makes it possible to retrieve conversations (from applications such as Skype or WhatsApp) and data stored in a computer system.
  - This makes it possible to remotely search a terminal's hard drive for information useful for legal investigations. Computer data are captured either by means of a technical device inserted directly into the medium or by remote injection.
  - The measure differs from the interception of electronic communications in that it targets computer data of any kind, not just written or sound messages.

- Germany: covert remote search of information technology system
  - Measure is defined in Section 100b of the StPO.
  - It may be used to access an information technology system used by the person concerned and data may be collected from that system (covert remote search of information technology systems), even without the knowledge of the person concerned.
  - It is understood to mean the online extraction of electronic storage contents that are not the primary subject of ongoing communication. This is done by searching storage media (e.g. the hard drive), i.e. searching existing databases for content stored there, such as text files, images, e-mails already received or sent and stored on the target system.
  - The measure is conducted by a software specially designed for this purpose. It must be ensured technically that only changes to the information technology system are made that are indispensable for data collection and that the

[39] Andorra, Argentina, Australia, Belgium, Brazil, Canada, Czech Republic, Denmark, Estonia, Finland, Georgia, Germany, Hungary, Iceland, Latvia, Lithuania, Montenegro, Netherlands, Nigeria, Norway, Spain, Türkiye, USA.

[40] Georgia also requires data subject notification for this power after a year elapsed.

changes made are automatically reversed when the measure is terminated, insofar as this is technically possible.
- In addition, there are data integrity and logging obligations.
- The software can also be introduced into the target system via the Internet if this is technically possible. The provision does not permit the clandestine entry into a home for the purpose of inserting the program into a computer.

- Netherlands: lawful hacking power and remote access with prior judicial authorisation based on lawfully obtained credentials [41]

  The Computer Crime Act III sets out a statutory basis for the "hacking power" in the DCCP (Sections 126nba, 126uba and 126zpa DCCP or Article 181 jo 126ng DCCP with prior judicial authorisation).
  The new investigative power allows specific designated law enforcement officials 'to covertly access computerised systems {automated works}[42] remotely, under certain conditions, that are used by suspects, with a view to certain investigative objectives in the area of the investigation of serious criminal offences'.
  After accessing a computerised system (such as a mobile phone or a server) the police may carry out a number of investigative activities, namely:
  - A) establishing specific characteristics of the computerised system or of the users thereof, such as their identity or location, and documenting such details;
  - B) executing an order to record confidential communications or wiretapping and recording communications;
  - C) executing an order for systematic observation;
  - D) documenting data stored in the computerised system; and
  - E) making data content inaccessible.

4.1.5 Competent authorities that authorise and carry out a search

Party	Competent authority that authorises a search	Competent authority that carries out a search
Albania	Judge	Prosecutor, Judicial police, expertise may be involved
Andorra	Investigating judge	Police officers and specialised authorities appointed by the investigating judge
Argentina	Judge	Prosecutors and police officers
Armenia	Judge	Police officers and technical experts
Australia	Judge or Administrative Review Tribunal (ART) member	Law enforcement authorities, including constables or constables assisting
Austria	Prosecution authority	Criminal investigation authority
Azerbaijan	Judge, Investigating judge	Law enforcement authorities with technical expert assistance
Belgium	39bis, § 2, paragraph 1: judicial police officer; 39bis, § 2, subparagraph 2: public prosecutor; 88ter: investigative judge ; 90ter: investigative judge.	Police experts

[41] For conditions for deployment of the measure and safeguards for persons as well as steps typically taken to execute the lawful hacking power, please see individual reply on Q 2.1.4 provided by the Netherlands.

[42] In the Computer Crimes III Act computerized systems are described as "automated devices/data carriers".

Party	Competent authority that authorises a search	Competent authority that carries out a search
Bosnia and Herzegovina	Judge	Prosecutors and police authorities assisted by computer forensics and digital forensics experts
Brazil	Judge	Police officer with technical expert (to ensure the chain of custody), prosecutor with technical expert, specialised units within police and prosecutorial services
Bulgaria	Judge	an investigator, an investigating police officer or an investigating customs officer. Other computer expert may be present
Cabo Verde	Judge, Prosecutor	Judiciary Police or any technician or expert authorised
Cameroon	State counsel, examining magistrate	Prosecutor
Canada	Judge	Peace officer, public officer, technical expertise may be involved
Colombia	Judge	Judicial police
Costa Rica	Judge	Prosecutor's Office and/or the Judicial Police
Croatia	Investigating judge, judge	Police officer and other specialised authority
Cyprus	Judge	Police officer
Czech Republic	Judge	Police officer
Denmark	Judge	Danish national police
Dominican Republic	Judge	Prosecutor, specialised cybercrime police
Estonia	Prosecutor	Experts and other technical experts
Fiji	Judge	Police and technical experts
Finland	Judge, prosecutor, police officer	Police authorities and other technical experts
France	Judge	Prosecutor, police officer, deputy prosecutor. Qualified persons to carry out technical examinations. Searches of special premises may be conducted by a magistrate.
Georgia	Magistrate	Specialised investigators or regular investigators with assistance of technical specialists
Germany	Judge	Police, custom or tax authorities. Other persons, such as interpreters, experts and expert witnesses may be involved
Ghana	Judge	Police or law enforcement officers, technical and other experts
Greece	Judge, prosecutor	Law enforcement officials, experts in digital forensics, cybersecurity, legal matters, and technical operations
Grenada	Magistrate	Police officers
Hungary	Judge, prosecutor, investigating authority	Prosecutor, Police and National Tax- and Customs Authority as investigating authorities, consultants with specific expertise
Iceland	Judge	Police authorities
Israel	Judge	The National Police, the Tax Authority, the Military Police, the Department of Internal

Party	Competent authority that authorises a search	Competent authority that carries out a search
		Police Investigations, the Securities Authority, the Competition Authority, and the Data Protection Authority
Italy	Prosecutor	Police forces and other law enforcement agencies
Japan	Judge	Public prosecutors, public prosecutor's assistant officers or judicial police officials
Kiribati	Judge	Police officer
Latvia	investigating judge	Specialised personnel
Liechtenstein	Investigating judge	Digital Crime Unit of Liechtenstein's National Police
Lithuania	Judge	Pre-trial investigation officer or the prosecutor, IT specialists
Luxembourg	Investigating judge, prosecutor	Police
Malta	Magistrate	Police officers
Mauritius	Judge	Investigatory authority
Monaco	Judge, prosecutor	State police (Cybercrime unit)
Montenegro	Investigative judge	Police officers, officers of the Digital Forensic Centre
Morocco	Investigative judge (if the investigation is opened), prosecutor (during the investigation phase)	judicial police officer
Netherlands	Judge, prosecutor, police officer (under certain circumstances also the police may carry out the search without authorisation and thus upon their own discretion)	Prosecutor and police officer. IT experts
Nigeria	Judge	Police
North Macedonia	Judge	Prosecutor and law enforcement officers
Norway	Judge, prosecutor	Police, prosecutors and related personnel
Panama	Judge, prosecutor	Prosecutor
Paraguay	Judge	
Peru	Judge	Prosecutor, National police
Philippines	Judge	Law enforcement officers
Poland	Judge, prosecutor	Prosecutor, police officer
Portugal	Judge, prosecutor	Prosecutor, police officer, specialised experts
Republic of Moldova	Investigating judge, prosecutor	Prosecutor, law enforcement officers
Romania	Judge	specialist working with the judicial bodies, external specialist or a specialized police officer, prosecutor or a police officer investigating the case
San Marino	Judge	Police officer
Senegal	Investigating judge, prosecutor	Investigating judge; police under supervision of prosecutor or investigating judge

Party	Competent authority that authorises a search	Competent authority that carries out a search
Serbia	Judge	Police
Sierra Leone	Judge	Law enforcement officer
Slovak Republic	Judge, prosecutor	Forensic technicians or experts
Slovenia	Judge	police officer
Spain	Judge	police officer, forensic engineering laboratories
Sri Lanka	Magistrate	Police officers, forensic experts under police supervision
Sweden	Investigation leader, prosecutor or judge	Investigating authority in cooperation with the experts in digital forensics or other specialized personnel
Switzerland	Judge, prosecutor	Police officer, other specialised authority
Tonga	Magistrate	Police
Tunisia	Judge, prosecutor	Police officer
Türkiye	Judge	Law enforcement units
Ukraine	Investigating magistrate, judge	Investigator, prosecutor
United Kingdom	Magistrate	Police officer
United States of America	Judge	Law enforcement officer

4.2 Implementation of Article 19.1 – Assessment

Answers to the following questions of the questionnaire were assessed:

- Q 2.1.1 Please summarise the legislative and other measures your country has undertaken to ensure that authorities can search or similarly access computer systems, data and data-storage mediums in your territory as described in Article 19.1. In answering, please summarise the requirements to be met and the procedural steps typically taken to obtain the authorisation for such a search.
- Q 2.1.2 Do particular rules apply in an emergency or other urgent circumstances? If so, please describe those rules and the applicable understanding of what constitutes an emergency.
- Q 2.1.3 Does your legislation empower your competent authorities to search or similarly access a computer system and data therein using lawfully acquired access credentials? In answering the question please summarise the requirements to be met and the steps typically taken to execute the power.
- Q 2.1.4 Does your legislation empower your competent authorities to search or similarly access a computer system and data therein using covert remote access? In answering, please summarise the requirements to be met and the steps typically taken to execute the power.
- Q 2.1.5 Which are the competent authorities that authorise and that carry out a search as described in Article 19.1? What type of technical or other expertise is required and utilized?

Party	Legislative and other measures	Assessment
Albania	Albanian legislation, in its Article 208/A of the Criminal Procedure Code (hereinafter the "CPC"), provides that it is the court that authorises the search and access to computer systems or parts thereof, upon the request of the prosecutor. In its decision, the court specifies the computer system (or part of it) to be accessed, the right to enter (access) the computer system, to search within the computer system, and to obtain the requested computer data. The public prosecutor or the judicial police officer ordered by the public prosecutor shall then execute the decision. When executing the order, the public prosecutor may appoint an expert who has special knowledge of the functioning of computer systems or measures for the preservation of computer data. The Albanian CPC does not contain definitions in general, which includes the definition of stored computer data. this is why in applying this article the definition used is the definition of the Budapest Convention. The Budapest Convention is ratified and is a part of the Albanian legislation, the interpretation of "computer data", is based on the definition of the Budapest Convention, in	Albania applies specific search and seizure powers to implement Article 19.1.

Party	Legislative and other measures	Assessment
	accordance with the article 116 of the Albanian Constitution, which states that international agreements ratified by Albania are enforced within the Albanian jurisdiction. Albanian legislation does not provide for special rules applicable in cases of emergency or other urgent circumstances. There is also no specific provision regarding access to the system using the access data, but Article 208/A of the CPC provides that the court shall grant the right of access and search in its decision. Albanian legislation does not provide procedural powers for covert remote access. Albania indicated that its legislation provides that the court is the competent authority to authorise search and seizure. The prosecutor makes the request and is then responsible for enforcing the court's decision by ordering the judicial police and, if necessary, appointing the expert.	
Andorra	Andorran search law derives from the Constitution, numerous articles of the criminal procedure code, and Law 22/2022 of 9 June regarding electronic systems. The criminal code also includes definitions and other relevant provisions. In sum, a search must be necessary, proportionate and suitable for the purpose. Its authorisation (by a judge) must be specific, well-founded in law and fact, and relate to major or certain minor crimes. Various criminal justice officials or a private party may seek such an order. In urgent circumstances, a search may take place if it has been verbally authorised by a judge (tribunal de garde) who later memorialises the authorisation in writing. Emergencies include when a target is hiding in a location or is found in the process of committing a crime. Lawfully obtained credentials may be used. The judge will closely scrutinise how they were procured. The search will otherwise follow the procedures described above. The police will take technical measures to ensure that others cannot use the credentials to affect the data to be searched.	Andorra applies general search and seizure powers to implement Article 19.1. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.

Party	Legislative and other measures	Assessment
	Covert remote access per se is not mentioned in Andorran law. However, in the case of certain crimes. the criminal code permits a judge to appoint a covert police agent, who could act with regard to electronic systems. Searches are authorised by juges d'instruction. Searches are executed by specially-trained or -educated police pursuant to international standards (ISO27001 and RFC3227).	
Argentina	The authorities of Argentina reported that its territory is composed of 23 provinces and the Autonomous City of Buenos Aires. Each province has its own local criminal procedure code, as does the City of Buenos Aires. These codes coexist with a criminal procedural code for the prosecution of crimes under federal jurisdiction. This federal procedural system is in a transitional period between two criminal procedure codes: the National Criminal Procedure Code (CPPN) and the Federal Criminal Procedure Code (CPPF) which is being implemented gradually with the idea that it will replace the previous one in the whole territory. Art. 151 of the CPPF provides for specific search and seizure power. Pursuant to this provision the judge may order, at the request of a party and by a reasoned order, the search of a computer system or part thereof, or of a computer or electronic data storage medium, in order to seize the components of the system, obtain a copy or preserve data or elements of interest to the investigation. It should be noted that there are specific provisions in place providing for search and seizure of stored computer data in some provincial codes and Argentina mentioned in its response which provinces have implemented specific provisions, these provisions were detailed in each case (the legislation of some of the provinces, which is more specific than the federal law, may be of interest). Several provinces have recently followed or plan to follow suit, which is commendable. However, Art. 151 applicable at federal level is not yet in force in the whole country. In this sense, it is important to note that the new Criminal Procedure Code introducing the adversarial system of criminal prosecution and its implementation is being carried out progressively throughout the country by a Bicameral Commission of the parliament in charge of the process of monitoring and implementation of the new procedural system.	Argentina has introduced specific search and seizure powers to implement Article 19.1. not yet applicable in the whole country. In the meantime, in practice Argentina applies a combination of general and specific search and seizure powers to implement Art. 19.1.

Party	Legislative and other measures	Assessment
	In Argentina, the so called "principle of evidentiary freedom" also applies, both to the search and seizure and to the chain of preservation of digital evidence (collection - storage - retention - production - presentation - evaluation of electronic evidence). The National Code of Criminal Procedure, the Federal Code of Criminal Procedure and the existing Protocols are applied in the federal jurisdiction. Article 224 of the CPPN also provides for the plain view doctrine that admits the initiation of an investigation if evidence of a crime other than the one investigated is found in a search, and it also extends to electronic evidence. There is no mention of the use of access credentials by authorities in compliance with the law. Remote access is only regulated in some jurisdictions, because in Argentina the provinces can regulate their procedural codes. The judge orders and the public prosecutor's office will execute the order together with the different specialized offices of the police forces that intervene for the fulfilment of the measure.	
Armenia	Article 236 of the Criminal Procedure Code provides for electronic searches and seizures in the territory. A court decision (a judicial warrant or order) is required to obtain authorisation for a search/seizure pursuant to Article 19.1. investigators execute the search/seizure and are assisted if necessary, by technical experts. There are no specific provisions regarding emergency or urgent circumstances. Armenia's legislation empowers the authorities to search or access computers using lawfully acquired access credentials. Beyond acquiring the credentials lawfully, the authorities must also have legal authority for the access, typically obtained through a judicial warrant or order. Technical means or specialised tools may be used to execute the access. There is no particular legislation permitting the use of covert remote access, but, in practice, it may be carried out.	Armenia applies specific search and seizure powers to implement Article 19.1.

Party	Legislative and other measures	Assessment
	There are no internal standard operating procedures or similar guidelines.	
Australia	Australia's response relates only to Commonwealth-level law. Australia relies on a general search statute and a computer-specific statute. The Crimes Act 1914 is the source of a range of search and seizure powers, including warrant processes, judicial approvals and handling of seized evidence. The Surveillance Devices Act 2004 covers surveillance devices and covert access to data in computers. This latter act establishes a regime for computer access warrants and the necessary predicate offences. "Stored computer data" are defined in one statute, the Telecommunications (Interception and Access) Act 1979. In addition, text in both the Crimes Act and the SD Act helps to define the concept. The warrant-related provisions of the Crimes Act lay out the requirements for notifications when premises or persons are searched. Both acts require that warrants be issued by a member of the judiciary (which includes various officials within the judiciary). Both acts define emergencies and provide that, in urgent circumstances, authorisations may be obtained under expedited procedures or searches may be conducted without a warrant. In the second case, post facto approval must be obtained. Certain warrants allow law enforcement to obtain information – for example, a passcode - that will allow access to data. Beyond this, when certain offences are under investigation, account takeover warrants may be obtained that allow changes to access credentials. More-extensive investigation requires a complementary warrant. Remote covert access may be authorised by warrant for more-serious offences. Notification of the search to the occupier of the searched premises may be delayed but should normally take place within six months. Searches are carried out by authorised law enforcement officers, who may be members of a number of (specified) Australian forces.	Australia applies a combination of general and specific search and seizure powers to implement Art. 19.1.

Party	Legislative and other measures	Assessment
Austria	Several sections of the Criminal Procedure Code provide for the search and seizure of objects including data storage media. All data accessible via data storage media may be searched, including when the data is password-protected and, in some cases, when cracking software is necessary. There is an obligation on the part of the person in possession of the item or data (limited if an accused is involved) to assist the authorities. The obligation extends to assistance with granting access to digital information the making of back-ups, etc. Generally, an order from the prosecution authority must be obtained; in some cases, the criminal investigation authority may seize objects on its own initiative. In some cases, higher procedural requirements obtain. Seizures are carried out by criminal investigative authorities, some of which are specially trained. In cases of "imminent danger" when there is an "unavoidable need for immediate intervention," the criminal investigative authority may act on its own initiative but must seek post facto prosecutorial approval. Covert remote access is not possible.	Austria applies a combination of general and specific search and seizure powers to implement Article 19.1.
Azerbaijan	The legal basis for searching and seizing computer data is primarily established by the Code of Criminal Procedure. The powers for search and seizure apply to offences against or by means of computer as well as other offences if evidence is electronic. Articles 177 and 242-247 of the CPC are the governing articles. There are no specific notification requirements. As a general rule, a court order is required to carry out searches and seizures in advance. Exceptionally, however, the investigative procedures may be carried out by reasoned decision of the investigator in circumstances that do not allow delay, in accordance with Articles 177.3.1, 177.3.2, 177.3.4 and 177.3.5 of the CPC (interception of telephone or other conversations and of information sent by means of communication media and other technical means). In addition, Article 243. 3 of the Code of Criminal Procedure stipulates that the investigator may carry out a search or seizure without a court order only if there is precise information indicating that objects or documents hidden in a residential building are evidence of the commission of a crime or of preparations for the commission of a crime against a person or the state; a person who has prepared or committed an offence against a person or the state, or a person who has escaped from a remand facility or prison is hiding in a	Azerbaijan applies general search and seizure powers to implement Article 19.1. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.

Party	Legislative and other measures	Assessment
	residential building; a human corpse (or parts of a corpse) is in the building; there is a real danger to the life or health of a person in the building. Execution of the search is restricted to the parameters in the order. Only the State Security Service and Ministry of Internal Affairs conduct searches in cybercrime cases. In other types of cases, those offices, several other law enforcement agencies, and the prosecutor's office conduct searches. Units specialising in digital forensics have been in place in the Ministry of Justice, Ministry of Internal Affairs and State Security Service for many years. These units are responsible for executing digital forensic investigations and handling digital evidence in cases involving stored computer data. Internal guidelines have not been adopted. Several CPC articles apply to emergencies or urgent circumstances. If investigative actions (as enumerated in certain CPC sections) cannot be postponed in urgent cases, the investigator must fulfill the obligations set out in Article 443.2, and, per another article, document them and justify their necessity and the impossibility of delaying the investigative action to obtain a court decision. An investigator may conduct a search or seizure without a court order in an emergency if specific information indicates certain circumstances (spelled out in the responses). In such cases, the investigators must write a decision justifying the need for the search or seizure in accordance with Article 243.4 and inform the court and the prosecutor within 24 hours and submit all supporting and related materials within 48 hours to the court exercising judicial supervision and the prosecutor to seek validation of the search action. If the court agrees with the investigator's position, it will issue an order validating the investigation. The legislation does not explicitly empower the authorities to use lawfully acquired access credentials. The general rules for search and seizure apply in such cases; thus it appears that lawfully acquired access credentials may be used in some cases. The legislation does not explicitly provide for covert remote access.	
Belgium	There are four bases for search and seizure: a police search in the course of an investigation, particularly an arrest, which may be done without prior prosecutor or judge authorisation; a search	Belgium applies specific search and seizure powers to implement Article 19.1.

Party	Legislative and other measures	Assessment
	without a seizure (for example, in a cybercafe), which requires prosecutor authorisation; a search, authorised only by a juge d'instruction, that may be extended to an accessible location other than the one being searched if two prerequisites are met; and a search, authorised only by a juge d'instruction, that is necessary to the proof. In addition, proportionality or potential loss of evidence must be in issue. Searches are executed by police experts. The law does not contain a definition of emergency, but a prosecutor or juge d'instruction may verbally order a search of data seized in an investigation. Such an order requires prompt post facto written justification. Lawfully acquired credentials may be used. The normal rules apply. Article 90ter of the criminal code provides for remote covert access under certain restrictive conditions, including that no other investigative method will suffice and that the search is being conducted to obtain proof, not for general investigation.	
Bénin	In general, searches and seizures derive their legal basis from the provisions of the CPC of Bénin. More specifically, search and seizure of stored computer data are governed by Articles 587, 590 and 592 of Law Number 2017-20 of 20 April 2018, the digital code act. Those provisions specify the means and conditions for searches and seizures, the competent authorities, and the cases in which copying data is desirable. The search and seizure powers are available for matters involving crimes against or committed with the use of information systems as well as crimes under Beninese law that entail electronic evidence. The authorities competent to authorise a search are the juge d'instruction and the Special Prosecutor of the economic crime and terrorism court (cour de répression des infractions économiques et du terrorisme (CRIET)). As a mandatory condition for a valid search, searches must be executed by officers of the judiciary police. Officers of the judiciary police who work on digital searches and seizures have been granted national jurisdiction by the court of appeals in Cotonou. These officers report to the CRIET prosecutor and have the correct equipment and means of transport to protect the integrity of the evidence collected.	Bénin applies a combination of general and specific search and seizure powers to implement Article 19.1.

Party	Legislative and other measures	Assessment
	Article 77 of the CPC and Article 589 of the digital code law require that searches and seizures be carried out only with the express consent of the person at the location of the operation. Such consent must be noted in the record of the operation. In addition, targets are requested to supply access credentials or information (also to be noted in the record). If targets decline to cooperate, the juge d'instruction or court may authorise access using any method. Article 589/2 provides that, if the crime involved carries a sentence of more than five years' imprisonment, or if the search merits it, the juge d'instruction may by written order authorise a search and seizure absent the consent of the person involved. Cases are considered urgent if a target is in a position to damage or destroy data that may contain evidence. In such cases, the normal search rules may be altered, and a search may be initiated before an approval is obtained from the Special Prosecutor of CRIET. Authorities may use lawfully-acquired access credentials to search a system also beyond an initially-searched system. Searching the system beyond an initially-searched system can be done without any further authorisation from the judge or the public prosecutor, for example on the basis of the provisions of the CPC (e.g. Articles 40, 76, 99). There is no provision for covert remote access. Internal guidelines or standard operating procedures have not been created.	
Bosnia and Herzegovina	The responses from this Party derived from four sources – Bosnia and Herzegovina, the Federation Bosnia and Herzegovina, Republika Srpska, and Brcko District. Their criminal codes and criminal procedure codes regulate procedures in nearly identical ways. The criminal code of Republika Srpska specifically reaches data that are the result of electronic data processing, computer systems, data storage devices and mobile telephones. Police or prosecutors apply to a court for a warrant, specifying the justification for it, providing details, and meeting the prerequisites, including the standard of reasonable suspicion that the targeted data relates to a	Bosnia and Herzegovina uses a combination of general and specific search and seizure powers to implement Art. 19.1. It appears that Bosnia and Herzegovina may not have fully implemented Article 19.1. Specific provisions establishing a legal framework of searches and seizure of computer data and systems applicable in all of the entities of Bosnia and Herzegovina could permit greater clarity and enhance legal certainty.

Party	Legislative and other measures	Assessment
	criminal offence. In several situations, such as in cases of likely danger to life or health or danger of destruction of evidence, the police or prosecutors may use non-formal methods – for example, phone calls or emails - to request authority to search and seize data without a written court order. Such actions must be reviewed and ratified within 48 hours. In Republika Srpska, an oral request for a warrant may be submitted when there is a risk of delay. In such cases, the approving judge will issue the same type of order as in routine cases. Urgent cases include those in which there is a risk that evidence will be hidden or destroyed, that another crime will be committed, that the target will flee, or that a person may be endangered. In the Federation Bosnia and Herzegovina, the current legislation does not provide for conducting computer seizures, given that each manipulation needs to be clearly described. Since they cannot be clearly described, they are not possible. The legislation in Bosnia and Herzegovina does not specifically empower the authorities to use lawfully acquired credentials (although undercover investigations, wiretaps, and other forms of surveillance may be authorised if properly justified). Under the CPC of Bosnia and Herzegovina, it is not clear if covert remote access is permissible. Covert remote access is not also possible under the CPC of the Federation Bosnia and Herzegovina. Per the Federal Police Administration, under the current legislation, there is no possibility to conduct undercover remote computer access given that each manipulation needs to be clearly described. Since the access cannot be clearly described, the measure is not possible. Article 234 of the CPC of Republika Srpska authorises covert remote access. Assuming that court authorisation has been procured, the police and/or prosecutors carry out the search. They are required to have specific technical knowledge and are often assisted by other technical experts. Overall, the search must be conducted pursuant to CPC rules to ensure that human rights are respected and that the evidence is admissible at trial.	

Party	Legislative and other measures	Assessment
Brazil	The legal basis for the search and seizure of stored computer data is established by the Brazilian Constitution, the Code of Criminal Procedure and the "Brazilian Civil Rights Framework for the Internet". There is no specific provision dedicated to the issue of data search and seizure. Rather, searching and seizing stored computer data is governed by the analogical application of the traditional search and seizure rules. The rule giving grounds to such a measure is Article 240 of the Code of Criminal Procedure, which encompasses stored electronic data, as no specific rule on the criminal procedure code exists. This Article allows the search and seizure of data, including stored computer data, with the authorisation of a judge and only in the cases and in the manner prescribed by law. The jurisprudential decisions in this matter state that Article 240 is sufficient to search and seize stored electronic data since once this measure is granted, the disclosure of the data is a consequence of it. Emergency or other urgent circumstances: The Brazilian courts have interpreted the concept of emergency broadly, recognizing that the protection of human life and physical integrity is a fundamental right that can justify the search or seizure of property without a court order. In addition, the Brazilian Code of Criminal Procedure provides that the authorities may search or seize property without a court order in cases of "caught in the act crimes" or when there is imminent danger to life or physical integrity. There is also a concept of "urgency" defined in the Civil Procedure Code, which also applies to criminal proceedings when there is evidence of the probability of the existence of the right and of the risk of damage or risk to the useful outcome of the proceedings (Art. 300). Brazilian legislation does not specifically authorise competent authorities to search or similarly access a computer system and the data contained therein using lawfully obtained access credentials. However, if the access credentials have been obtained by lawful means, such as a court order or search warrant, the competent authorities may use them to access a computer system and the data contained therein, subject to the requirements and procedures established by Brazilian law.	Brazil applies general search and seizure powers to implement Article 19.1. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.

Party	Legislative and other measures	Assessment
	This legislation does not specifically empower competent authorities to search or similarly access a computer system and the data contained therein by means of covert remote access, but the Prosecutor General has recently filed for an injunction in the Supreme Court regarding this matter to recognize the need for regulation and call on Congress to act. Authorities must obtain a court order or warrant to search or seize computer data, as required by the Brazilian Constitution and the Code of Criminal Procedure (CCP). This must be authorised by a court order or search warrant. The court order or warrant must be based on reasonable suspicion of the commission of an offence and must specify the location of the search, the type of data or information to be accessed, and the time frame for the search. Authorities must use covert remote access strictly in accordance with the conditions set out in the court order. This measure must be authorised by a Judge in a well-grounded decision at the Prosecutor's request, or endorsement when the request comes from the police. However, in general, the Police is the authority to implement the measure, and a technical expert is required to ensure the chain of custody, the Prosecutor is also entitled to implement the measure, also accompanied by a technical expert. The authorities also clarified that the Budapest Convention entered into force in Brazil as ordinary law in April 2023 and based on that, in combination with Art. 240 of the CCP it provides a legal basis for the investigation and prosecution concerning electronic evidence of any crime. It should be noted, however, that the procedural powers set out in the Convention are formulated in a way that requires further implementation through domestic law. They cannot function properly if their corresponding text is simply reproduced in domestic legislation. Further specification under domestic law is needed, for example, in relation to the competent authorities, as the powers in the Convention do not specify what the competent authorities are to be, and it is for each Party to clarify these specifics in its domestic law.	
Bulgaria	According to Articles 160 through 162 of the CPC, searches must be done through a prior court authorisation. If this is not possible in urgent cases, authorisation shall be obtained within 24 hours. Searches and seizures related to computer information systems and software products must be carried	Bulgaria applies specific search powers to implement Article 19.1.

Party	Legislative and other measures	Assessment
	out in the presence of a technical expert. Article 163 of the CPC prescribes detailed procedures for searches and for collection and proper storage of evidence. Authorities may ask a user of a computer system to provide access credentials, However, there is no explicit legal obligation for the user to provide them. (under Article 159 of the CPC, there is an obligation to produce objects, papers, computer information data and other data that may be important for the case) Covert remote access is not provided for.	
Cabo Verde	Cabo Verde has informed that its National Cybercrime Law (hereinafter the "CL"), no. 8/IX/2017, addresses the matter of computer data search. Article 17º provides that if it becomes necessary to produce evidence to discover the truth during a process, specific and determined computer data stored in a particular computer system can be obtained. The competent judicial authority authorizes or orders a search to be carried out in that computer system, and should, whenever possible, preside over the diligence. As judicial authorities, both the judge and the Public Prosecutor's Office can authorize or order a search, depending on the procedural phase. The evidence obtained must be necessary for the investigation, and the computer data in question must be specific and determined. The Cape Verdean legislator has allowed criminal police bodies to conduct searches without prior authorization from the judicial authority. However, this is only possible under two conditions: i) The person who has control of the data consents to the search, and the consent is documented; ii) In cases of terrorism, violent or highly organized crime, when there is well-founded evidence of the imminent commission of a crime that puts the life or integrity of any person at serious risk. However, in both cases, you must prepare a report and send it to the relevant judicial authority. If you are dealing with paragraph iii), you must immediately inform the competent judicial authority for validation purposes. If there is a founded reason to believe that a crime is about to be committed and that this crime poses a serious risk to the life or integrity of any person, the criminal police may carry out a search without prior authorization from a judicial authority.	Cabo Verde applies specific search and seizure powers to implement Article 19.1

Party	Legislative and other measures	Assessment
	Cabo Verde has stated that there are no specific provisions for searching or accessing a computer system and its data using lawfully acquired access credentials. Cabo Verde has stated that there are no specific provisions for search or similar access a computer system and data therein using covert remote access. Depending on the procedural stage, the Judge or the Public Prosecutor's Office may authorize searches. However, even during the investigation phase, the Public Prosecutor's Office must obtain authorization from the judge to access e-mail messages or similar communication records. The criminal police body, usually the Judiciary Police, or any technician or expert entrusted with the task, searches. Technical knowledge is required to carry out the search.	
Cameroon	Preliminarily, it should be noted that Cameroon is continually developing its legislation on cybercrime/cybersecurity to make it as comprehensive and all-encompassing as possible. The legal bases for the search and seizure of stored computer data are: - Article 29 of the Cybercrime and Cybersecurity law No. 2010/012 of 21 December 2010, which states that "(1) Operators of information systems shall be obliged to keep connection and traffic data from their information systems for a period of ten (10) years. (2) Operators of information systems shall be obliged to install mechanisms for monitoring and controlling access to data from their information systems. Stored data may be accessible during judicial investigations. (3) The installations of operators of information systems may be searched or seized by order of a judicial authority under the conditions provided for by the laws and regulations in force"; and, - Article 41 of the same statute, which states that "everyone has the right to respect of his privacy. Judges may take precautionary measures, in particular sequestration and seizure, to prevent or to stop an infringement of privacy". Search and seizure powers also apply to offences under statutes other than the Cybercrime and Cybersecurity law if evidence is on computer systems.	Cameroon applies a combination of general and specific search and seizure powers to implement Article 19.1.

Party	Legislative and other measures	Assessment
	Articles 29 and 41 empower the judicial authorities to search, access and even seize computer systems and stored data. All this is done in compliance with the conditions defined by the laws and regulations in force. Article 93 of the Criminal Procedure Code requires the authorities to have a warrant for this purpose. There are no special rules for domestic emergencies or other urgent circumstances that are domestic. Searches using lawfully acquired credentials are permitted when the authorities have a warrant obtained by the state counsel (procureur de la république) in accordance with the provisions of the CPC. Searches using covert remote access have not been provided for by the law. The state counsel or the examining magistrate (juge d'instruction) authorise and carry out searches. Cameroon does not yet have internal standard operating procedures or search guidelines, but it has initiated the drafting of a digital investigation procedures manual to better address digital investigations in general and searches and seizures of computer data in particular.	
Canada	The default requirement for a police search is judicial authorisation, normally via a general warrant under section 487 of the Criminal Code. Subparagraphs of Section 487 of the Criminal Code provide specific authority for electronic searches. A general warrant is appropriate for the search of a computer or electronic device. General warrants may be permissible when investigators need to use innovative techniques that are not specifically mentioned in the code. The notice requirements associated with a computer search derive from other sources of law. Searched persons are either aware that a search is being conducted or are advised of it by a copy of the warrant; for that reason, notification is not addressed by the code. It is the judiciary that authorizes searches and seizures (justice of the peace, a provincial court judge or a judge of a superior court of criminal jurisdiction). To issue a warrant, a court must be satisfied that there are reasonable grounds to believe that an item being sought relates to, or will provide evidence of, an offence or that one of several other bases for a warrant has been fulfilled. A warrant may then be issued to a peace officer (or a public officer, in certain cases), who will execute it. Executing officers may have completed basic or advanced computer forensic training.	Canada applies a combination of general and specific search and seizure powers to implement Article 19.1.

Party	Legislative and other measures	Assessment
	A search may be conducted without a warrant in exigent circumstances if it would be impracticable to obtain a warrant. The legality of such a search will be tested against the Supreme Court's reading of Canada's Charter of Rights and Freedoms. An exigent-circumstances search will be permissible only if there was an "imminent danger of the loss, removal, destruction or disappearance of the evidence if the search is delayed" or if there is a degree of urgency that necessitates action by law enforcement. An extensive body of law exists in this area. Lawfully-acquired access credentials may be used, assuming that the proper authorisations – which may vary – are procured. Covert remote access is available pursuant to a general warrant.	
Chile	Chile does not have an express provision on the search and seizure of computer data and media containing computer data. Nor do the rules referring to the search of physical spaces and the seizure of physical elements mention computer devices or data. It appears that in practice, the provisions of the articles of the Code of Criminal Procedure may perhaps be used by analogy. The Chilean report notes that according to their legislation (art. 12 law 21.459), when the investigation of certain specific computer-related offences established in the said law becomes essential and there is a reasonable suspicion, based on concrete facts, that a person has committed or participated in the preparation or commission of any of the offences established in the said provisions, the judge of guarantees, at the request of the Public Prosecutor's Office, which must submit a detailed preliminary report on the facts and possible involvement, may order the application of the techniques provided for and regulated in articles 222 to 226 of the Code of Criminal Procedure, in the manner established by this Regulation. In relation to emergencies or other urgent circumstances, Chile pointed out that there are no special rules for these cases.	Chile applies general search and seizure powers to implement Article 19.1. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.

Party	Legislative and other measures	Assessment
	Current legislation does not give specifically power to search a computer system and its data, or to gain similar access, using legally obtained access credentials. Covert remote search can be executed pursuant to newly adopted Art. 225 bis of the CPC. The provision authorises the use of computer programs that allow remote access and apprehending the content of a device, computer or computer system, without the knowledge of its user. The measure may be applied only for 30 days, the guarantee judge may extend this period for periods of up to the same duration, with a maximum of 60 days.	
Colombia	The Criminal Procedure Code (Criminal Procedure Code) or CPP (Law 906 of 2004), precedes Colombia´s accession to the Budapest Convention. Nevertheless, the Colombian procedural dispositions endorse the probative value of digital evidence and allow the identification, extraction, and conservancy of digital evidence through integration of various general and special norms about the matter. The Office of the General Attorney informs that article 236 of law 906 of 2004 allows the extraction of digital evidence stored in information systems, communication devices, or destined for data transmission, when there is notice that these have a relation with the commission of any crime, or the suspect has transmitted or stored information of interest to the case. When the prosecutor reasonably suspects that the accused is manipulating data through telecommunication networks, they shall order the judicial police to retain relevant information and equipment for forensic analysis to obtain evidence. Colombia also provided jurisprudence establishing that this type of rule applied to the collection of any electronic or digital document, like digital evidence stored in computer systems, cellular phones, and other types of systems. Also, it established that the formalities to order such extraction of information only require subsequent judicial control by a judge of control of guarantees. According to article 221 of the Colombian Code of Criminal Procedure, there must be a well-founded motive or probable cause that justifies obtaining digital evidence stored on a device on the grounds that this evidence: i) the commission of an act or ii) makes its commission more probable. The order of extraction is emitted and signed by the incumbent prosecutor of the case, in a written manner and directed to expert judicial police in computing forensics by a term that can vary from 30 to 15 days	Colombia applies general search and seizure powers to implement Article 19.1. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.

Party	Legislative and other measures	Assessment
	depending on the case. The seizure referred to in this article shall be limited exclusively to the time necessary to capture the information contained therein. The seized equipment shall be returned immediately, if necessary. Colombia did not provide rules in an emergency or urgent circumstances. However, it has been explained that in the framework of the competencies of the Judicial Police, electronic evidence collected in urgent acts that are executed during the attention to a crime scene (in which case a warrant to the judicial police is not required, for example, during the inspection of the scene of the crime). Colombia has not specific measures to ensure search or similar access to a computer system data therein using legally acquired access credentials. Finally, it has not developed legislative capacities related to access a computer system and data therein using cover remote access credentials.	
Costa Rica	The seizure of the hardware containing the electronic data can be ordered by the prosecutor or Judicial Police to protect the evidence, however in order to search and analyse the data, an order by a Judge is required, also, even though the seizure itself of the hardware can be order by the prosecutor or judicial police, if its (the hardware) located in a private space (houses, non-public workplaces, etc.) you must also get a Judge order to grant you permission to access to the private space in which the hardware is located. There are no rules for emergency cases; however, situations regarding threats to the life or integrity of people or the security of the nation, are processed expeditiously according to the emergency or urgency of each specific case. Also, investigations affecting victims of vulnerable groups have a priority of resolution. There is no specific requirement regarding the "notification" of the order, the executing authority will give a copy of the order to the owner, custodian or any person that is in the same place in which the hardware containing the data is.	Costa Rica applies general search and seizure powers to implement Article 19.1. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.

Party	Legislative and other measures	Assessment
	There is no specific legislation regarding search or access to a computer system using legally acquired credentials. Costa Rica has no legislation regarding covert remote access to a computer system to obtain information for a case. The competent authorities in Costa Rica to access an information system to obtain computer data, in application are the criminal judge who orders the access, and the Prosecutor's Office and/or the Judicial Police that executes the order. Costa Rica has not specifically regulated digital evidence. Rather, it applies the same provisions that were designed for physical evidence by analogy.	
Croatia	A search of movable property also includes computer and devices connected with the computer, other devices for collecting, saving and transferring of the data, telephone, computer and other communications, as well as data carriers. Unless otherwise prescribed by the CPC, a search shall be ordered by a written warrant with a statement of reasons issued by an investigation judge. Pursuant to Article 242, Paragraph 4, of the CPC, the search shall be carried out by the state attorney or an investigator or police authorities. The term "investigator" refers to a public official who acts upon a warrant of the state attorney or investigative judge (police, military police, custom or tax administration officer). However, only the police authorities and police investigators are equipped with forensic tools and trained to carry out a computer search and in practice they conduct these measures. Exceptions to the requirement of a judicial warrant apply in cases of urgency described as "danger in delay". Articles 244 and 245 of the CPC describe in detail six circumstances under which searches may be conducted without an investigating judge's warrant and without delivery of other preliminary documents. These circumstances include expected armed resistance or other dangers to those executing the search, risk of destruction or concealment of evidence, and the necessity of surprise in certain cases.	Croatia applies specific search and seizure powers to implement Article 19.1.

Party	Legislative and other measures	Assessment
	Under Article 245, if delay would defeat the purpose of a search and the case involves one of the very serious crimes listed in the article, the search may be executed based on a state attorney's well-founded, written warrant. Within eight hours from the end of the search, the warrant must be submitted to the investigating judge, who must ratify or reject the search within eight hours. Persons using the computer are obliged to provide access credentials. Defendant (suspect) can do so on a voluntary basis. Further examples of cases without prior issuance of a warrant are provided for in Article 244, which provides for covert remote access. The term "covert remote access" is not explicitly described by law. It refers to the fact that a search, including on devices connected to the initially-searched system, could be carried out without informing the defendant or the owner/possessor of a searched object prior to the search. However, the mere fact that a search under Article 244 could be covert or extended to connected devices does not constitute its distinctive element: this measure could equally be carried out when the suspect is aware that it is taking place, despite non deliverance of the warrant or bill of rights, or when there are no connected devices.	
Cyprus	Cyprus utilises two elements of its law for electronic searches. First, Article 27 of its Criminal Procedure Law requires a search warrant or other court order, issued by a judge, based on a police officer's attestation to several procedural requirements. Second, when a court orders the search of private communications stored in a computer system, the elements of Article 23 of the Protection of the Privacy of Private Communications Law of 1996 must be fulfilled. The same requirements apply in emergencies. Because the system emphasises search warrants and court orders, its authorities do not rely on lawfully acquired access credentials except where consent to search has been obtained. Covert remote access is not authorised.	Cyprus applies general and specific search and seizure powers to implement Article 19.1. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.

Party	Legislative and other measures	Assessment
	As noted, searches must be authorised by a judge. They are conducted by the police pursuant to an internal digital forensics' manual. The personnel of the Cyber Crime Unit's Digital Forensic Lab are certified computer forensic examiners.	
Czech Republic	Search of the computer system and data stored therein is possible under the general powers for house search (Provision 83) and search of other premises and places (Provision 83a) both defined in the Criminal Procedure Code (CPC). Although the legislation does not explicitly define emergency, special regime can be applied to the measures of handing over an item, personal search and search of other premises and places in case that action has to be performed immediately. Such situation may occur, if there is a risk of damage, destruction, lost or hiding the item important for criminal proceedings. The legislation allows for the authorities to use lawfully obtained credentials. A person cannot be forced to hand over the credentials if such handling could breach the prohibition of self-accusation. It is also possible to search the computer system secretly pursuant to provision of 158d par. 3 of the CPC. Certain limitations apply (intentional criminal offence, proportionality, court order, timely limited duration of validity of the court order). The presiding judge and in pre-trial proceedings the judge upon a motion of the public prosecutor is entitled to order a house search. In urgent cases a house search may be ordered, instead of the competent presiding judge or judge (Section 18), by the presiding judge or judge, in whose jurisdiction is the house search to be performed. Same procedure applies for search of other premises and places. House search and search of other premises and places are performed by a police authority.	Czech Republic applies general search and seizure powers to implement Article 19.1. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.
Denmark	Supreme Court judgments have clarified that the statutory regime for non-electronic searches and seizures also covers searches and seizures of electronic systems and data. All are explicitly regulated at length in numerous sections of the Administration of Justice Act, and these sections impose additional restrictions on, and requirements for, these measures. Generally, both searches and seizures require a court order issued if the several elements specified in the AJA sections have been satisfied.	Denmark applies general search and seizure powers to implement Article 19.1. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.

Party	Legislative and other measures	Assessment
	If delay to obtain a court order would render the search pointless, the police may decide to conduct the search and/or seizure. In such cases, court ratification of the police decision must be requested within 24 hours. In both types of situations, the National Police execute the searches and seizures, employing the necessary technical expertise. Use of lawfully acquired access credentials is covered by the general rules on search. The responses appear to refer here to Sections 793 and 796 of the AJA, which provide that the police can search other objects and locations outside the house and that a decision to do so may be made by the police. A Supreme Court decision also allowed the use of lawfully acquired passwords. Covert remote access by the police is not included per se in statute. However, if certain requirements are met, the police may utilise Section 799 of the AJA in investigations of certain serious crimes. This section removes the notification and presence requirements that would normally apply to a search. It also permits the police to use a suspect's code and username to access an account or data remotely. Other provisions may also be relevant: "data reading" and "interference with correspondence" (which includes several types of electronic data), may be carried out secretly per Sections 791b, 783, and 784. See Denmark's extensive responses on this point.	
Dominican Republic	The Dominican Republic has Law 53-07 Against High Technology Crimes and Offences, where Article 52 refers to the Criminal Procedure Code, which establishes measures for registering and obtaining evidence. These measures also apply to obtaining and preserving data contained in an information system or its components, such as traffic data, connection, access, or any other useful information. Additionally, public prosecutors or police officials may conduct searches when there are reasonable grounds to believe that evidence useful for the investigation or concealment of the accused exists, following the rules and provisions of the criminal procedure code. In cases of urgency and the absence of the public prosecutor's office, the police may request it directly.	Dominican Republic applies a combination of general and specific search and seizure powers to implement Article 19.1.

Party	Legislative and other measures	Assessment
	Before carrying out the formalities provided for in the Code of Criminal Procedure, the Public Ministry may access or order access to such an information system or one of its components. It may also instruct persons with knowledge of the functioning of an information system or one of its components, or of the data protection measures in that system, to provide the information necessary for carrying out the relevant investigations. Procedural legislation of Dominican Republic does not provide for the possibility of using covert remote search techniques. However, it is important to note that there is currently a draft law in Congress to amend the Cybercrime law 53/07. The draft stipulates that these techniques would be allowed only in the case of serious offenses specifically set forth by the law. Searches can only be carried out at the request of the Public Prosecutor's Office, with a reasoned court order. This procedure is carried out by the Public Prosecutor's Office with the assistance of police officers specialising in cybercrime.	
Estonia	Generic powers concerning search as well as examination of an object are applied. There are general rules for emergency situations. In case there is an emergency then the Prosecutor's Office may give authorisation for the covert access to the computer system and court authorisation needs to be obtained in 24 hours. As a general rule the search can be authorised by the Prosecutor's Office. There is no specific legislation for using lawfully obtained access credentials. However, legislation does not preclude this, general powers for search and seizure are applied. Legal framework provides also for covert access to computer systems. Such measure requires authorisation by a judge.	Estonia applies general search and seizure powers to implement Article 19.1. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.
Fiji	Sections 16 and 21 of the Cybercrime Act (2021) (hereafter "TCA") provide for search and seizure of stored computer data. The Police/FICAC may apply for a warrant to a Judge/ Magistrate to search a computer, computer program, computer system or any part therein, computer data storage medium, computer data device, activate any onsite computer system & computer data storage. Section 21	Fiji applies specific search and seizure powers to implement Article 19.1.

Party	Legislative and other measures	Assessment
	provides that a warrant application must justify the need for the search and specify how it will be conducted technically. Fiji reported that emergency or urgent circumstances are both not regulated by the TCA. It appears that Section 21 may be used as a legal basis for the use of lawfully acquired access credentials. Authorities stated that Sections 22 and 23 of the TCA that allow for the collection of real-time collection of traffic data and interception of content data through a search warrant may be used also for the covert remote search. Authorisation by a judge is among the strict conditions that must be met in this respect. Additionally, Illicit Drugs Control Act provides that a High Court judge may, on the written application of a police inspector or senior customs officer, issue a warrant where there is reasonable suspicion that a person has committed, is committing or is about to commit an offence under the IDCA. This warrant allows for the covert monitoring and recording of communications, including telecommunications. The competent authority to authorize a search is a judge, and those who carry out the search are the police and officials with technical expertise.	
Finland	Legal basis for searching and seizing stored computer data is the Coercive Measures Act (hereinafter referred to as the "CMA") Chapter 10 of this Act contains provisions on covert coercive measures, while Chapter 5 of the Police Act deals with covert methods of intelligence gathering. The relevant provisions on searches are set out in Chapter 8 of the CMA. Sections 20-29 detail the requirements for searching data contained in a device. Searching data contained in a device means to accessing data stored in a computer, terminal equipment or other technical equipment or information system at the time of the search. However, confidential communications that are subject to interception, traffic data monitoring or technical surveillance in accordance with Chapter 10 cannot be searched.	Finland applies specific search and seizure powers to implement Article 19.1.

Party	Legislative and other measures	Assessment
	The CMA contains relevant provisions for the search and seizure of stored computer data. Chapter 7 specifies that the prerequisites for seizing objects or documents also apply to data contained in technical devices or information systems. Chapter 8 outlines the provisions for searching data in devices. Section 21 of chapter 8 stipulates the prerequisites for a search of data contained in a device. A search of data contained in a device may be conducted if: (1) there is reason to suspect that an offence has been committed and the most severe punishment provided for the offence is imprisonment for at least six months, or if the matter being investigated involves circumstances connected to the imposition of a corporate fine; and (2) it may be presumed that the search can lead to the discovery of a document or data to be seized. Furthermore, the decision on the conduct of a search of the premises may be extended to also cover a technical device or information system in said premises, if the search in question is not intended to find a person.	
France	Search and seizure procedures will vary according to the stage of investigation at which they take place – for example, there is a preliminary investigation stage. The procedures are therefore governed by differing sections of the CPC and may involve differing justice system officials. Judicial authorisation is required when a search concern any of seven specially-protected professions – for example, lawyers, notaries, and journalists – and for searches without consent at the preliminary investigative stage regarding certain crimes. Judicial authorisation is required for every use of a special investigation technique, according to Article 706-95-11 of the CPC. Per Article 706-102-1 of the CPC, the following are considered such special investigation techniques: setting up a technical device, without the consent of the persons concerned, for the purpose of accessing, recording, retaining and transmitting computer data in any place. This includes data stored in a computer system, displayed on a screen for the user of an automated data processing system, entered by the user by typing characters, or received and transmitted by peripheral devices. Three statutes provide for special procedures, including for data searches and seizures, without the participation of a judge when there is a threat to public order or of terrorist activities (with some exceptions for persons in certain professions, such as attorneys or journalists).	France applies specific search and seizure powers to implement Article 19.1.

Party	Legislative and other measures	Assessment
	The authorities may search a subsequent system that is accessible from an initially searched system. They may use lawfully acquired credentials. They may also use covert remote access, in particular against organized crime and terrorism. France's response details clearly the statutes from which these powers derive and the forensic techniques that are permitted. Generally, police officers (sometimes of a certain rank) conduct searches. Searches affecting persons in certain professions must be conducted by a magistrate. In a preliminary inquiry into a serious crime, a prosecutor may obtain a judicial order to conduct the search without the consent of the person searched. In cases that are at the preliminary investigation stage or where a juge d'instruction is already engaged, judges' orders will guide the searches. Forensic experts may be employed.	
Georgia	General rules of the CPC for search primarily designed for physical environment apply to search of stored computer data. Article 136 – Causing the disclosure of computer information or document applies mutatis mutandis. Court warrant is a prerequisite for search. Prosecutor must show to magistrate/judge that there is probable cause. Its requirements are provided by law. The law also provides for a different procedure under urgent necessity. In those cases, investigating officer may conduct search upon prosecutor's authorisation. Within 24 hours after completion of search and seizure prosecutor has to request court *ex post facto* authorisation. Investigation authority may search a computer system using lawfully acquired access credentials. Investigator and where needed other law enforcement officers and/or technical specialists execute search warrants. There is also a special procedural power of covert remote access to a computer system with a view to securing data under Article 143(1)b of the CPC, such measure is subject to court authorisation and limited to serious crimes.	Georgia applies a combination of general and specific search and seizure powers to implement Article 19.1.
Germany	General rules of the Code of Criminal Procedure provided for search and seizure of premises and persons are applicable (Section 102, 103, et seq, of the Code of Criminal Procedure). Part of these	Germany applies a combination of general and specific search and seizure powers to implement Article 19.1.

Party	Legislative and other measures	Assessment
	search measure is the inspection of identity papers and electronic storage media pursuant to Section 110 of the Code of Criminal Procedure. These measures allowing the examination is the instrument provided by law for checking the content of electronic storage. Searches pursuant to Section 102 of the Code of Criminal Procedure may only be ordered by the judge in accordance with Section 105 of the Code of Criminal Procedure; in exigent circumstances, they may also be ordered by the public prosecutor's office and its investigators. To obtain a search warrant, the public prosecutor files an application with the court. Urgent powers exist in the case of imminent danger. As a rule, imminent danger exists if the order cannot be obtained by the judicial authority without jeopardizing the purpose of the measure. The search order is generally executed by the public prosecutor's office, which in turn may mandate other investigating authorities (police, customs, tax authorities) to conduct the search. Authorities may use lawfully acquired credentials to access and search a computer system or data, to search or similarly access a computer system and data. Search Warrant or consent of the person concerned is needed. The covert remote search has a specific legal basis in Section 100b of the Code of Criminal Procedure. Pursuant to Section 100b (1), technical means may be used to access an information technology system used by the person concerned and data may be collected from that system, even without the knowledge of the person concerned, for specifically provided serious crimes and under other conditions provided by law. This measure of Covert remote search of information technology systems are understood to mean the online extraction of electronic storage contents that are not the subject of ongoing communication.	
Ghana	The constitution underlies search and seizure law in its protections of the right to privacy. Beyond this, three statutes are relevant. Generally (see exceptions below), the judiciary authorises searches and they are executed by law enforcement officers, when necessary with the assistance of several types of specialised third-party experts. Law enforcement agencies are likely to be responsible for authorising and executing searches that relate to cybercrime and computer data. Internal standard	Ghana applies a combination of general and specific search and seizure powers to implement Article 19.1.

Party	Legislative and other measures	Assessment
	operating procedures or guidelines have been adopted. There is no requirement that the interested party be notified of a search. The Criminal Procedure Act governs searches and seizures, permitting them based on a warrant issued by a magistrate. This warrant will issue after an ex parte application that includes sworn evidence of reasonable grounds for believing that a search will aid in investigating or preventing a crime. Searches and seizures may be conducted without a warrant when carried out incident to an arrest. Also, as detailed in Section 93, a police officer may conduct a warrantless search and seizure of a package or article in numerous circumstances. The procedures for procuring a warrant pursuant to the Cyber Security Act and the Electronic Transactions Act are similar to those under the CPA, but the application must be made to a higher court. Additional conditions must be met under the CSA (see Sections 71-74). The two statutes primarily provide the legal framework to deal with offences related to or committed using electronic systems. Those laws may not explicitly cover every possible offence. The application of search and seizure powers to computer evidence of offences that are *not* specifically related to computers can sometimes be complex. However, general principles of search and seizure could apply to evidence of non-computer-related offences. As detailed in the responses, various issues and requirements may come into play. There are no specific rules for an emergency or other urgent circumstances. However, the CPA permits warrantless searches incident to arrest. The Economic and Organized Crime Act also permits an authorised officer to conduct an emergency search and seizure when the officer has reasonable grounds to suspect that an item is tainted property or will provide evidence of a serious offence under that statute. Finally, there is a possibility pursuant to Supreme Court jurisprudence that evidence seized outside of established procedures might nevertheless be admissible. In certain cases, the authorities may use lawfully-acquired access credentials, presuming that the authorities have the legal authority to do so – for example, through a warrant or other court order –	

Party	Legislative and other measures	Assessment
	and that the access is necessary to procure relevant data. Numerous procedural requirements must be complied with. There is no specific legislation regarding covert remote access.	
Greece	Searches require prior authorisation by prosecutorial or judicial order after a showing of probable cause or reasonable grounds to believe that the data sought is relevant to a criminal investigation. Law enforcement agencies or investigative bodies are authorised to carry out searches, according to the scope and purpose in the order. Experts in digital forensics, cybersecurity, legal matters and technical operations may be involved in the execution of searches. The power to search and seize computer systems and electronic data applies to all offences. There are no special provisions for emergencies. The authorities are permitted to use lawfully acquired access credentials with legal authorisation, typically a judicial or prosecutorial order. Similarly, covert remote access may be used if a judicial or prosecutorial order is first obtained. In both instances, the actions of the authorities are restricted to the scope and purpose specified by the order.	Greece applies a combination of general and specific search and seizure powers to implement Article 19.1.
Grenada	The authorities reported that their legislation includes the Electronic Crimes Act, Section 22 of which outlines the powers of access, search, and seizure for investigative purposes (Art. 22). Grenada outlined situations that are considered as an emergency (kidnapping, threat or harm to person of national security interest, or threat or harm to a child), these may be detailed in the warrant authorised by a magistrate or judge. There is no power provided for by law to search or similarly access a computer system and the data contained therein by means of covert remote access.	Grenada applies specific powers to implement Art. 19.1.

Party	Legislative and other measures	Assessment
	The authorizing officer for the warrant must be a magistrate. Police officers of the rank of Inspector or above apply for and execute search warrants or appoint officers to execute such warrants.	
Hungary	Written orders to conduct searches and seizures may be issued by a court, prosecutor, or investigating authority. Several sections of the CPC relate to this issue and mention electronic data explicitly; searches may be ordered if their justifications meet specified standards. Notaries and attorneys receive special protections and the CPC emphasises the presence of the person involved or an adult substitute. According to several sections of the CPC, searches may be conducted without court orders if delay would significantly jeopardise the purpose of the search. Such searches must be ratified promptly by court post facto. Other coercive acts that would assist with a search may also be taken. Electronic searches are often deemed urgent due to the vulnerability of electronic data. Searches are executed by the police or another national law enforcement entity or the prosecution service. They have specially trained personnel but may employ expert consultants. The legislation neither prohibits nor authorises the use of lawfully obtained credentials. As a practical matter, investigators have lawful control of any seized devices and data, so the use of such credentials is possible (and must be recorded). Covert remote access is permissible and is specifically detailed in Sections 231-234 of the CPC, provided by Hungary in its answer.	Hungary applies specific search and seizure powers to implement Article 19.1.
Iceland	There are no particular and specialized legal provisions for search of computer systems or computer-data storage mediums specifically, but the legal basis for search can be found in Art. 74 of the Code of Criminal Procedure no. 88/2008 (CCP) which is a general provision for searches. The provisions of Article 75 of the CCP describe the procedural conditions that have to be met for a search to be granted. A court order is required unless the unequivocal consent of the owner or the person in charge of item has been given.	Iceland applies general search and seizure powers to implement Article 19.1. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.

Party	Legislative and other measures	Assessment
	Emergency is not defined by law, however if there is an imminent risk that waiting for a court order could result in damage to the procedure a search may be carried out without court order. This shall also apply if a search is being made for a person who is to be arrested and he or she is being followed, or there is a danger that he or she will escape if it is necessary to wait for a court order. It is common in practice, in line with principles on proportionality, to give owners or custodians of data contained on seized data carriers (devices) locked with PIN codes, passwords or similar (e.g. cell phones) the opportunity to supply police voluntarily with the relevant access credentials to open the device. It is understood by the authorities that covert remote access measures fall under the scope of Chapter XI. of the CCP on telephone tapping and other comparable measures. According to Art. 80 and 81, such operations can involve information from telecommunications companies on communications with a computer, including the tapping or recording of such communications. Following conditions apply: court order, presence of a lawyer when deciding on the measure, reason to expect that information of great significance for the investigation will be obtained that way, either threshold for offences (6 years) or list of offences to which the measure may be applied. Measures are carried out by police authorities, if needed with assistance from other specialised police authorities, for example, if operational or technical experience or expertise should require.	
Israel	Sections 23, 23A, and 28 of the Criminal Procedure Ordinance (Arrest and Search) as well as State's Attorney Guideline no. 7.14 and National Police Guideline no. 03.300.035 and Supreme Court jurisprudence govern searches and seizures in general and electronic searches in particular. Searches are authorised based on applications that fulfil numerous specific requirements. Warrants must be issued by a judge and contain details of the purpose of the search and its constraints. The search must be necessary and the infringement on the privacy of the person affected must be limited. The National Police and several other authorities have the power to carry out searches. Officials executing digital searches must have undergone specialised training.	Israel applies specific search and seizure powers to implement Article 19.1.

Party	Legislative and other measures	Assessment
	There are no special rules in emergencies; a judge is on call 24/7. Lawfully acquired credentials may be used pursuant to the framework described. The legislation does not authorise covert remote access.	
Italy	Italian legislation includes the following provisions in its Criminal Procedure Code: Article 247 - Search: A personal search is authorized when there is reasonable suspicion that an individual is concealing evidence or related items on their person. A local search is authorized when there is reasonable belief that evidence or items are located in a specific place or when the arrest of a suspect is feasible in that location. In cases where data or information relevant to a crime is suspected to be stored in a computer or telematic system, a search can be ordered, complemented by measures to safeguard the original data. Legislative amendments now extend inspection, search, and disclosure orders to computer data. Article 244(2) of the Code of Criminal Procedure has been updated. It empowers the Judicial Authority to investigate cases where a crime has left no physical evidence or where such evidence has been lost, deleted, altered, or dispersed. The authority can also order technical operations, including those involving computer and telecommunications systems, to preserve and protect original data. Emergency or other urgent circumstances: the judiciary police are enabled to proceed with requests to providers (according to art. 254-bis) a/o search and seizure activity, prior to the public prosecutor taking the lead of the investigation according to art. 352 -1bis and 354. According to the jurisprudence of the Supreme Court, the use of lawfully acquired access credentials to access a computer system and its data is recognized as a legitimate method of conducting searches. According to the jurisprudence of the Supreme Court, if the covert remote access is suitable to capture one live flow of communication between two or more subjects, that would fall under the lawful interception activity.	Italy applies a combination of general and specific search and seizure powers to implement Article 19.1.

Party	Legislative and other measures	Assessment
	Police forces and other law enforcement agencies can carry out a search upon authorization of the competent Judicial Authority = Public Prosecutor. Specific computer analysis and forensic skills are required.	
Japan	Articles 102 and 218 of the CPC cover searches. Prosecutors, public prosecutor's assistant officers or a judicial police officer must apply for and justify the issuance of a warrant by a judge. Electronic media as well as electronic data may be searched. The search is executed by prosecutors or judicial police officials. The officials executing electronic searches are technically qualified. Searches incident to the arrest of a person may be conducted without a warrant. It appears that covert remote access is not available in Japan. Lawfully acquired credentials may be used in searches that comply with Article 218.	Japan applies a combination of general and specific search and seizure powers to implement Article 19.1.
Kiribati	The Kiribati Cybercrime Act 2021 provides procedural powers for law enforcement to search and seize electronic evidence. There also exist procedural statutes such as the Kiribati Criminal Procedural Code and the Kiribati Police Powers and Duties Act 2008. While these statutes do not explicitly address the search and seizure of stored computer data, these statutes often aid search and seizure even for stored computer data. The procedural powers under the Cybercrime Act apply both to offences against or by means of computers and any other offences under domestic law where evidence is on a computer system. Section 22 of the Cybercrime Act provides that a court may issue a search and seizure warrant for computer systems, data, and storage media within Kiribati. To obtain the warrant, a police officer's application must satisfy the court that there are reasonable grounds to suspect that such items may be material as evidence in proving an offence under the Act or any other offence committed by means of a computer system or that they have been acquired by a person as a result of an offence.	Kiribati applies a combination of general and specific search and seizure powers to implement Article 19.1.

Party	Legislative and other measures	Assessment
	Police officers execute searches, per the Cybercrime Act. Intermediate to advanced level digital forensic expertise is required. Kiribati police officers need training and capacity building in this area as no formal courses are available to train Kiribati's police officers in cybercrime technical investigative skills. The government cybersecurity incident response team also has a legal mandate under the Digital Government Act 2021 to provide technical expertise when law enforcement requests such assistance. Section 25 of the Cybercrime Act outlines the procedures for emergency or urgent preservation of evidence when a law enforcement authority believes that there is a high risk of evidence being lost or rendered inaccessible. Per section 25, law enforcement authorities may issue a written notice to order retention for up to 60 days for such evidence. They may extend this up to 100 days. A court warrant is not needed. The procedural powers under the Cybercrime Act allow law enforcement authorities to use all necessary search measures, including the use of lawfully acquired credentials. However, these powers are only granted when a court issues a warrant for a search and seizure. Per section 22 of the Cybercrime Act, covert remote access can be used when the court has issued a warrant. Drafting of internal standard operating procedures is planned for this year based on regulations implementing the Cybercrime Act.	
Latvia	Several sections of the CPC regulate different types of searches and seizures, including specifically those having to do with electronic data and systems. Beyond ordinary searches and seizures, "special investigative actions" may be used in specific cases under Articles 210 and 212 of the CPC. Such actions are permitted only for certain crimes and based on the decision of an investigating judge (with some exceptions).	Latvia applies a combination of general and specific search and seizure powers to implement Article 19.1.

Party	Legislative and other measures	Assessment
	Per Article 180 of the CPC, in situations where evidence may be compromised or destroyed, searches may be done with the consent of the prosecutor but must be ratified promptly by the investigating judge. Lawfully acquired credentials may be used if examining and recording data is necessary and if the person affected is present. The usual search procedure is followed if the data must be extracted. Covert remote access is permissible with the authorisation of a judge. Articles 218-222 of the CPC detail the differing procedures. Ordinary searches and seizures must be authorised by an investigating judge or a court based on an application by the person directing the proceedings. They appear to be executed by investigating officials. Special investigative actions are authorised by the decision of an investigating judge and executed by state authorities that are specially authorised by law to do so.	
Liechtenstein	In general, to search and seize electronic media or data, prosecutors apply for an order from an investigating judge and the order is executed by the National Police, apparently by the Digital Crime Unit. Recent amendments to law make explicit that these powers extend to storage media and to data, including data protected by access keys, passwords, etc. The Police Act permits the police to act on their own initiative in cases of "imminent danger." The National Police may seize objects without a court order when data are at risk of being lost. Lawfully acquired access credentials may be used. Per Section 104b of the CPC, the National Police may use its officers or other persons in undercover investigations.	Liechtenstein applies a combination of general and specific search and seizure powers to implement Article 19.1.
Lithuania	Searches and seizures are addressed by several articles of the CPC. In general, a prosecutor applies for a court order, supplying a reasoned justification for the order, which may apply to objects and to	Lithuania applies general search and seizure powers to implement Article 19.1. Provisions specific to computer

Party	Legislative and other measures	Assessment
	computer data. The order is executed by the pretrial investigating officer or prosecutor. IT specialists may assist. Examination of the data is done by specially educated and -equipped law enforcement personnel. The CPC permits searches and seizures without court authorisation in "urgent" cases, where there is no immediate possibility of obtaining court authorisation and the evidence is at risk of loss. Several consequences follow if the search or seizure is not ratified by a judge within three days, including that the evidence must be destroyed and is unusable at trial. Access credentials may be used if lawfully acquired in the course of a pretrial investigation. Covert remote access is permitted as outlined in the CPC, particularly in Articles 158 and 160.	data and systems could permit greater clarity and enhance legal certainty.
Luxembourg	Various enumerated articles of the Luxembourg CPC, primarily Articles 31, 33, 63-66 and 88-1 through 88-4, form the legal basis for searches and seizures as envisioned by Article 19. Depending on the circumstances, such measures are authorized either by the Public Prosecutor or the Investigating Judge and are carried out by the police. Articles 34 and 63 of the CPC establishes the right of the accused and counsel and the civil party to be present at a search. However, their presence may be dispensed with when there is reason to fear "the imminent disappearance of elements whose discovery and examination seem useful for establishing the truth." In case of search and seizure at a third party's place (e.g. seizure of a domain name at the national domain provider) or during the analysis of the seized data by the Judicial Police, only the Police is present. According to the detailed text of Article 31 of the CPC, in the case of a "flagrant crime," the police have the responsibility (in summary) to ensure that at-risk evidence is preserved, including by seizure. Although not specifically provided for in the CPC, lawfully acquired access credentials procedural measures under several provisions of the CPC may be applied (Art. 33-38 and Art. 63-68). Covert remote search is possible through special investigative measures (Art. 88-1 through 88-4).	Luxembourg applies a combination of general and specific search and seizure powers to implement Article 19.1.

Party	Legislative and other measures	Assessment
Malta	General and computer-specific articles of the Criminal Code regulate the power of the police to execute searches with and without a warrant issued by a magistrate. Once within premises, the police may seize anything that they reasonably suspect is connected to a crime (among other conditions) and to prevent data from being altered, destroyed, concealed, etc. The police may also require computer data to be delivered in portable, visible, and legible form. There is no notification regime. The powers relating to search and seizure of computer data may be applied with regard to any domestic offence. Several subparagraphs of Article 355E of the Criminal Code specify the circumstances under which a warrant is not necessary for a search. They include that a) the offence is a serious crime and 1) there is a present and imminent danger that the target may abscond or 2) there is a clear possibility that evidence will be tampered with or destroyed; b) the target is caught during the commission of an offence; c) immediate intervention of the police is necessary to prevent the commission of a serious crime; and d) the action is in connection with arresting fugitives under certain circumstances. The Malta Police cannot use lawfully acquired access credentials to conduct investigations or conduct covert remote access investigations. Such actions would constitute criminal offences. Magistrates authorise searches, which are executed by the police force.	Malta applies a combination of general and specific search and seizure powers to implement Article 19.1.
Mauritius	Searches as described in Article 19.1 are governed by Section 28 of the Cybersecurity and Cybercrime Act 2021. They are authorised by judges based on sworn ex parte applications demonstrating reasonable grounds for the issuance of a warrant. Warrants are executed by an "investigatory authority," so this power is not vested in a particular authority. Section 28 does not specify any emergency exceptions to the normal procedures. However, applications for warrants could explain that the circumstances are urgent. The same section provides an investigating authority the power to extend a search if data is lawfully accessible from the initial system (within Mauritian territory).	Mauritius applies specific search and seizure powers to implement Article 19.1.

Party	Legislative and other measures	Assessment
	No current legislation permits the use of covert remote access. The specialised officers of the police IT unit execute the examination; local or foreign expertise can be called in when needed. The standard operating procedures of the police include guidelines regarding the handling of evidence. There are no established procedures within the Cybercrime Unit, but officers are trained to international standards. The IT Unit in the police is ISO-certified and has internal working instructions and guidelines based on international standards.	
Monaco	Three (listed) sets of laws govern searches and seizures. In particular, law number 1.435 of 2016 regarding electronic criminality provides for searches of computer systems, data, and data storage media. This law introduces into the CPC the specific procedural powers of the BC. The requirements are the same as those for seizures in any criminal case. The power to search and seize computer data applies to all offences. Searches and seizures should be authorised by a prosecutor or judge. Execution will be carried out by the Cybercrime Unit of the state police. Monegasque legislation contains provisions for responding to emergency situations in cases of flagrant crime or misdemeanour (art. 266 of the CPC) or urgent interceptions (art. 106.4. of the CPC) without specifically defining emergency or urgent cases. Domestic law authorises competent authorities to use lawfully acquired access credentials to conduct investigations or conduct covert remote access investigations. Covert remote access is not provided explicitly by the domestic law. Nevertheless, the authorities can carry out data interception or use of qualified agents.	Monaco applies a combination of general and specific search and seizure powers to implement Article 19.1.

Party	Legislative and other measures	Assessment
Montenegro	The legal basis for search of stored computer data is provided by Criminal Procedure Code. In particular, Art. 75 provides for Search of dwellings and other premises. Its para 2 covers the search of computers and similar devices for automatic data processing. An investigative judge issues a search warrant and the police officers execute a search warrant. Article 78 regulates grounds for a request for search to be made in verbal form in case of urgency (the risk of delay) of the search exists. The risk of delay always means that if certain actions are not conducted immediately, there is a danger that the evidence will not be able to be obtained later or may be lost or compromised. Any person shall enable access to the computer and removable storage used for storing information relative to the object of the search (discs, USB flash discs, USB hard discs, diskettes, tapes etc.), as well as give necessary information on the use of the computer. The CPC under the chapter 9 regulates measures of secret surveillance. This measure can be used only in relation to certain offences and under special circumstances. The search is carried out and managed on the spot by an investigative authority – an investigator, an investigating police officer or an investigating customs officer.	Montenegro applies a combination of general and specific search and seizure powers to implement Article 19.1
Morocco	Legislative amendments to the CPC are under consideration in the legislature that will affect the law of search and seizure and related issues in this questionnaire. For that reason, Morocco's responses must be considered provisional. At this moment, the search of stored computer data is regulated by general rules on search, without discriminating specifically which may correspond to electronic evidence and stored electronic data. Searches of papers, documents, or other objects may be undertaken either by the police when a crime has been interrupted or, in most cases at the preliminary investigation stage, with the explicit consent of the person concerned and the authorisation of the competent public ministry. Once the case has reached the charging stage, a juge d'instruction may order a search. The judiciary police execute searches.	Morocco applies general search and seizure powers to implement Article 19.1. It is in the process of updating its legislation and, in the meantime, its criminal procedure mechanisms are close in practice to the requirements of the Convention. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.

Party	Legislative and other measures	Assessment
	In terrorism cases, the hours in which a search is permissible may be extended if the investigation requires it. In cases of extreme urgency, or if the loss of evidence is feared, searches may be conducted with the written authorisation of the public ministry. The questions regarding the search using lawfully acquired access credentials and the search using covert remote access did not have a response.	
Netherlands	Powers for searching computer data have been introduced in the Criminal Procedure Code when the Netherlands ratified the cybercrime convention (2006, Computer Crimes II Act). Criminal procedure code introduced in art. 125i DCCP the power to search in a computer system or part of it and computer data stored therein or a computer-data storage medium in order to preserve data. In practice such a computer search is combined with a home search and general rules regulating the search of premises apply. The power may only be executed when there is a reasonable expectation that the search will produce relevant information for the investigation. The power is executed mostly upon issuance of an order by a public prosecutor, and sometimes pre-validated by an investigative judge. Criminal Procedure Code authorities to search or similarly access a computer system and data therein using lawfully acquired access credentials (Art. 125i, 125k of the DCCP). In this regard, legitimately acquired credentials are understood as gaining knowledge of credentials by the execution of another procedural power such as testimony. Pursuant to Art. 126bb paragraph 1 of the Criminal Procedure Code there are different obligations for the public prosecutor to inform in writing the person against whom a special investigative power has been exercised. The written notification to a person involved is made as soon as 'the interest of the investigation' allows it. A standard provision elaborated by the Public Prosecutor's Office regarding “standard operating procedures”, is in force.	Netherlands applies specific search and seizure powers to implement Article 19.1.

Party	Legislative and other measures	Assessment
	In case of urgent circumstances, related to a reasonably expected disappearance of evidence, and when the arrival of the investigative judge cannot be awaited the prosecutor may conduct the search (Art. 97 of Criminal Procedure Code). The Criminal Procedure Code also introduced in 2019, measures to "covertly access computerized systems remotely".	
Nigeria	Three statutes provide the primary bases for electronic searches. Generally, Section 29, Police Act, 2020 and Sections 143 and 144 (searches) and section 333 (seizures) of the Administration of Criminal Justice Act, 2015 (ACJA) provide the legal justification for searches and seizures under Nigerian laws, including searches and seizures of electronic data. In both, a police officer applies to a court for authorisation of a search or seizure. The third statute, the Cybercrimes Act, specifies in detail the ex parte application, the offences for which warrants will be issued, the powers that may be authorised, and the requirement of reasonable grounds to believe that the data sought will be relevant. Pursuant to its Section 45, searches are authorised only by a court and are executed by the police. Nigeria has laws other than those above that deal with various offences in which data and other electronic evidence are necessary in obtaining preservative orders from the courts or in proof of elements of the offence. These laws may also outline specific procedures for search and seizure of electronic data when dealing with offences under those laws. For example, sections 58(1) and 58(2)(d) of the Nigeria Data Protection Act, 2023, provide for search and seizure of data and electronic evidence and the procedure is similar to that of section 45(1) of the Cybercrimes Act. Every investigative agency that has the power to conduct searches has adopted internal standard operating procedures. Section 45 (1) is expected to be used in emergencies, since warrants are procured by ex parte application. For example, in cases involving minors, formal processes will be dispensed with. Section 45(1) envisages cases of (extreme) emergency or urgency. For clarification about how the section is	Nigeria applies a combination of general and specific search and seizure powers to implement Article 19.1.

Party	Legislative and other measures	Assessment
	applied, Nigeria provided an illustration (arising from a live case). A network service provider (C) facilitates the communication between device A and B and the communication is aimed at interfering with the computer or network system of a public institution in Nigeria. Pursuant to section 39 of the Cybercrimes Act, C has intercepted the communication and informs the law enforcement agency (ICPC). At this point, C avails all the information at its disposal about device A and B, including location and records of the communication, to the ICPC. Then an officer of the ICPC approaches the court ex-parte, with a statement on oath, for an order to search the premises and seize devices A and B. Both the use of lawfully-acquired credentials and covert remote access are possible pursuant to Section 45. Under an order pursuant to section 45(2)(f)(g) of the Cybercrimes Act, an officer is lawfully empowered to "use any technology to ..." (f) or "require the person having charge of ..." (g) to input the credentials and then have the requisite access. Section 45(e) provides for cases where a covert remote search would be applicable.	
North Macedonia	Several CPC sections cover traditional and, separately, electronic searches and seizures. Generally, a prosecutor applies to a court for a warrant, but the police may apply for a warrant if there is a danger of delay. In either case, if the warrant is granted, the search is executed by the prosecutor and police. Specialised technical police may also be involved. In any of the four types of emergencies defined in Article 191 of the CPC, a search may be executed without a warrant and without certain other procedural protections. One of the types of emergencies is a risk of destruction of traces of the crime or objects important to the proceedings. Use of lawfully-acquired access credentials is not defined in the CPC, but the CPC describes a sufficiently broad way in which evidence can be obtained, so live forensics can be used as a tool. According to Art. 184 para. 1 and 2 of the CPC, in connection with Article 192 and 195 para. 1, 2and 3 and Art. 198 para. 1, 2 and 3 of the CPC, there is a possibility of live forensics. Any person carrying out the procedure must be licensed to use the tool involved and must be able to show the authenticity of all actions taken. Under Article 184, computer users or those with access must "give all necessary information required for unobstructed fulfilment of the goals of the search." Further, the case example provided in response to question 2.2.6 indicates that credentials may be used to extend a search.	North Macedonia applies a combination of general and specific search and seizure powers to implement Article 19.1.

Party	Legislative and other measures	Assessment
	Covert remote access is permissible under Article 252 of the CPC, "Purpose and types of special investigative measures." Such access may be used only when no other method of obtaining the evidence will suffice. The Ministry of the Interior sends a request to the Public Prosecutor's Office, which sends it to the court. A court will issue the order for the special investigative method for a specific period of no more than one year. The order will be re-evaluated within 30 days.	
Norway	The applicable Norwegian CPC sections cover all searches and seizures, not electronic data specifically. Absent the written permission of the person concerned, a court order is generally needed beforehand. Some types of electronic data, including subscriber data, may be available without a court order. In some urgent cases, a prosecutor may order a search and seizure without a court order, per the CPC, but the decision must be recorded and explained promptly. A police official may conduct the search and seizure of objects, etc., without a court order in certain limited circumstances, including the discovery of fresh evidence during a search. A prosecutor must ratify this decision as soon as possible. Beyond these circumstances, there is another very small sphere of possible use of police procedural powers in emergencies. It appears that lawfully acquired access credentials may be used within certain specified limits if their use is proportionate to the facts of the case. Covert remote access in the form of reading data is permitted as described in two sections of the CPC. It must be authorised by a court and is available only in relation to certain crimes. Prosecutors seek court authorisation for searches and they are executed by prosecutors and police officers, including with the assistance of technical experts. Extensive technical training is included in Norwegian police training.	Norway applies general search and seizure powers to implement Article 19.1. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.
Panama	In Panama, the legal basis for the seizure of stored computer data is Article 314 of the Criminal Procedure Code, which authorises the prosecutor to seize data as part of an investigation. The seizure of private correspondence or documents requires the prior authorisation of the judge of guarantees,	Panama applies a combination of general and specific search and seizure powers to implement Article 19.1. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.

Party	Legislative and other measures	Assessment
	based on Article 310 of the Code of Criminal Procedure. This provision applies to all devices, not just electronic ones, making it the legal basis for accessing any device to search for private documents. After seizing the device, support or storage medium, the defense must be notified, but their presence is not mandatory. If there is an immediate need to access and search the devices, the defense must be present. The seizure of data is subject to subsequent supervision by the judge of guarantees, who must respect professional secrecy and the confidentiality of documents. The law does not provide for emergency cases, as post-seizure supervision is always required anyway. Article 310 of the Code of Criminal Procedure allows the Public Prosecutor to act in emergency situations under the subsequent supervision of the Judge of Guarantees. These emergencies include preventing crimes, responding to requests for assistance, apprehending individuals in the act of committing a crime, preserving evidence, and conducting procedures immediately after a search. Panama does not mention the possibility or impossibility of searching or accessing a computer system with legally obtained access data. In addition, it is important to note that the Code of Criminal Procedure establishes the principle of freedom of evidence. In this country, there's no reference to the concept of covert remote access. The competent authorities that authorise and carry out a search in accordance with the provisions of Article 19.1 are the Public Prosecutor's Offices that make up the Public Prosecutor's Office, as the body that directs the criminal investigation. If it is a seizure of data, the corresponding legalization must be requested from the Judge of Guarantees, within a period of 10 days, for the judicial use of this data to proceed, and if it is confidential information, such as communications or private data, prior authorisation is required from the Judge of Control of Constitutional Guarantees.	
Paraguay	Paraguay informed they apply the modifications of the Paraguayan Criminal Code, Law No. 4439/2011 which "amends and expands various articles of law no. 1160/97 "criminal code", and the procedural norms provided for in article 192 of technical operations and article 200 of intervention of communications and article 214 of the Paraguayan criminal procedure code. Paraguay has established its powers through freedom of evidence, in Article 173 of the Procedural Code, which operates with	Paraguay applies general search and seizure powers to implement Article 19.1. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.

Party	Legislative and other measures	Assessment
	the principle of search for the truth, regulated in Article 172 of the Procedural Code. It is a general rule for all types of evidence. There is not a specific regulation that includes specific rules that are the subject of digital evidence, there are only good practices by the Public Ministry, such as the application of principles of expertise, regarding the chain of custody, etc. The determination of "urgent circumstances" in Paraguay depends on specific cases and the violation of legal rights, particularly if cybercrime perpetrators are caught in the act. Consequently, both the Public Ministry and the National Police are obligated to act. Paraguay's criminal code includes a legal provision for the jurisdictional advance of evidence to request urgent expert opinions. Article 217 outlines the process, where experts are selected and appointed by the judge or the Ministry Public during the preparatory stage, unless it involves jurisdictional advance of evidence. Additionally, Article 320 addresses the jurisdictional advance of evidence, allowing for essential activities like recognition, reconstruction, inspection, or expertise that are considered definitive and irreproducible, or when obtaining a statement during the trial is deemed difficult due to obstacles. To carry out these actions, court orders are necessary, and they are requested by the Public Prosecutor's Office. In cases involving digital evidence, under the principle of freedom of proof, the Public Prosecutor's Office must accurately describe the investigated facts and the technology involved as a means to commit the alleged acts. Consequently, they are required to specify the potential digital evidence that the Judge needs to order for seizure. There is no mention of the use of access credentials by authorities in compliance with the law. Remote access is not yet authorised. The competent authorities that authorise the searches are the Criminal Guarantee Judges and the Permanent Attention Criminal Judges who have material and territorial jurisdiction.	
Peru	Search and seizure are regulated in article 217 of the Criminal Procedure Code and Law 27697. The measures that restrict rights are applied to register or similarly access computer systems, data and data storage mediums in the territory. Regarding the requirements to be met: In accordance with numeral 1 of article 203 of the Criminal Procedure Code, the seizure must be motivated under the requirement of the "proportionality" test and under the requirement of the "sufficiency of evidential	Peru applies general search and seizure powers to implement Article 19.1. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.

Party	Legislative and other measures	Assessment
	elements" test: a) Regarding "proportionality", the restrictive seizure measure must pass this test considering the criteria established in national jurisprudence. b) Regarding the "sufficiency of evidential elements", the restrictive seizure measure must pass this test with the analysis of the elements that provide relevant evidence for the investigation, which start from the initial suspicion and that can arrive. Article 217 of the Criminal Procedure Code specifies that during an "inspection," a term related to a "search" (as per paragraph 191 of the Explanatory Report of the Budapest Convention), real coercive measures can be carried out through "seizure." This includes the confiscation of items that could serve as evidence or be subject to confiscation. These measures must be accurately documented and appropriately identified, with the chain of custody maintained. This allows "seizure" to be considered as a complement to the execution of an "inspection." It's important to note that "seizure" is not the same as "inspection" or "search." The latter term falls into a similar category as the terminology used for searches, data reviews, or inspections, as per paragraph 191 of the Explanatory Report of the Budapest Convention. No specific rules apply in case of emergency or other urgent circumstances. On the other hand, in case of being caught in the act, measures restricting rights such as seizure are subject to judicial validation. The use of legally acquired access credentials for registration or access is not a mandatory requirement for each of the rights-limiting measures at present. This absence of a requirement does not imply that if access credentials are obtained, for instance through the voluntary submission by the access credential holder for the purpose of registering or accessing a computer system and its data, they cannot be employed. Current legislation does not prohibit the voluntary provision of access credentials by the holder, as it falls within their right to manage the data they deem appropriate. In practice, during the execution of an "inspection" and the subsequent "seizure" of goods, there may be situations in which the owner of the goods (electronic devices) willingly provides passwords or access patterns, demonstrating their clear intent to cooperate. Such actions are documented in the corresponding record of seized property, which may or may not be carried out, and this decision does not impact the execution of the measure, nor does it affect potential future judicial validations, if applicable.	

Party	Legislative and other measures	Assessment
	Remote access has not been regulated and has not been discussed yet. The restrictive seizure measures are required by the Prosecutor, authorised by the Judge through a duly reasoned resolution, and executed by the Prosecutor and/or the National Police, the personnel that executes the measure must have minimally basic computer knowledge to carry out a successful search.	
Philippines	Searches are authorised by warrants, which are issued by judges after a finding of probable cause based on a verified and substantiated application and affidavits. These preliminary documents must state the underlying basis for the search and specify the search and seizure strategy in detail. Law enforcement units that specialise in cybercrime and digital forensic analysts execute searches that involve electronic data. Search and seizure powers apply to all offences. There are no special rules for emergencies. Use of lawfully acquired access credentials is permitted pursuant to the power to order any person to provide information to facilitate searches and seizures. Covert remote access is not available.	The Philippines applies specific search and seizure powers to implement Article 19.1.
Poland	A court or public prosecutor issues decisions authorising searches except in the urgent cases described below. The CPC prescribes numerous conditions for electronic searches pursuant to the general rules on search and seizure and pursuant to rules specific to electronic proceedings. These conditions include requirements of documentation, presence of persons affected or suitable substitutes, etc. Searches may be executed by a public prosecutor or by the police or officials from a specialised authority, depending on the relevant statute or court or prosecutor order. Forensic technicians complete specialised training. If data is retained and examined, the examination should be conducted by officers within certain police or forensic units.	Poland applies a combination of general and specific search and seizure powers to implement Article 19.1.

Party	Legislative and other measures	Assessment
	Urgent situations are defined as those in which delay could lead to the loss or alteration of evidence or leads – for example, if switching off a system in the course of a seizure will cause the loss of data. In such cases, a search may be executed, but the unit conducting the search must produce a warrant from the head of the unit or an identity card. Thereafter, the search must be ratified by a court or the public prosecutor. The person concerned must be notified of the right to a decision, must receive it within seven days, and has additional rights in such situations. It appears that searches may be extended using lawfully-acquired credentials when this is documented. Police guidelines also authorise the use of computer devices or programs giving access to data that is encrypted or protected by a password, including where such measures are used for equipment connected to the initially-searched item. The Polish Code of Criminal Procedure does not contain explicit regulations regarding remote searches of an IT system or covert remote access. However, covert remote access seems to be permissible. Such a search may be authorised by a court or prosecutor, depending on the stage of the proceedings, the act to be performed and the type of data sought. Forensic technicians or other experts execute the access.	
Portugal	Searches and seizures are regulated not by the general regime of the CPC but by the provisions of the Cybercrime Law, Law no. 109/2009, as amended. Under this system, searches may be undertaken when authorised by a prosecutor in the investigation phases or by a judge in later phases. Those authorities should be present at the execution of the order, if possible. In most cases, the actual execution is carried out by the police and, as necessary, by additional experts. There is no statutory provision concerning emergencies, but Portugal intends to ratify the Second Additional Protocol, which implies that emergencies will be included in a future domestic law. However, the police may execute a search without prior judicial authorisation 1) with the voluntary, documented consent of the relevant person, or 2) in investigations of certain serious crimes, when there is well-founded evidence of an imminent crime posing a serious risk to a person's life or health. In such cases, to preserve the admissibility of the evidence, the search must be documented and promptly ratified by the appropriate authority.	Portugal applies specific search and seizure powers to implement Article 19.1.

Party	Legislative and other measures	Assessment
	The use of lawfully acquired credentials and covert remote access are not foreseen in the law.	
Republic of Moldova	Moldova relies on several general statutes for searches of electronic data. These powers apply to all offences in the criminal code. Searches are authorised by an investigating judge (or, in the urgent cases described below, by a prosecutor). The searches are executed by law enforcement and/or the prosecutor (one or the other is necessary, but both may be present). Forensic specialists may be involved. The General Prosecutor's Office has adopted cybercrime investigation guidelines. Article 127 of the CPC addresses the presence during the search of the searched person or various possible representatives. Beyond this, there are no specific notification requirements in the CPC. "In cases not subject to postponement or in cases of flagrante delicto," pursuant to Article 125 of the CPC, searches may be conducted based on a reasoned order of a public prosecutor, not the investigating judge, subject to that judge's ratification of the action within 24 hours. Pursuant to a search warrant and Article 125 of the CPC, law enforcement may access data using lawfully acquired credentials. Covert remote access may be utilised pursuant primarily to a 2023 statute and Article 138 of the CPC.	Moldova applies general search and seizure powers to implement Article 19.1. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.
Romania	Searches and seizures are authorised by the appropriate court (which may vary) after application by a prosecutor. The prosecutor or investigating police officer will be present at the execution of the warrant, as will the defendant and possibly a defence attorney. Actual execution of the warrant is carried out only by technical specialists attached to the judicial authority or by specialized police. If a defendant is in custody, then the presence of defence counsel at the search is mandatory. There are no special rules for emergencies. However, if it is determined during a search that the target data are in a system or storage medium accessible from the initial searched item, the target data are copied and preserved and application is made to extend the warrant. Lawfully acquired credentials may be used. Suspects and defendants are not obligated to reveal credentials.	Romania applies specific search and seizure powers to implement Article 19.1.

Party	Legislative and other measures	Assessment
	According to art.138 para 1 let. b) of RO CPC under a court order competent authority can access covertly a computer system directly or remotely. This power is a surveillance measure performed covertly using lawfully acquired credentials and it is different than the computer search provided by art.168 CPC.	
San Marino	San Marino stated that there is currently no specific legislation on search and seizure of stored computer data. It was also indicated that the case-law has not been yet largely developed when it comes to matters related to computer data. It appears that analogous legal principles are applied largely. Also, the authorities informed that the Supreme Court of Appeal has ruled on the acquisition of computer data in criminal proceedings (Judgement no. 8 of 15 November 2021). This process involves several stages: first, a physical search of the devices containing the data, followed by a computer search to extract the relevant information, and finally, the seizure of this data on a preliminary basis. If an immediate computer search is not possible for technical reasons, the physical device or a complete forensic copy is seized for further analysis. The seizure order must be specific and must state exactly what data is being sought and for what investigative purposes. Searches may be carried out by judicial police officers, either by delegation from the judiciary or on their own initiative in case of urgency and necessity. Article 78 of the Code of Criminal Procedure legitimizes searches stating that the police must act with due caution and collect both incriminating and exculpatory evidence. Cases of urgency: The San Marino authorities indicated that if it is not possible to wait for a court order, Article 58-duodecies of the Code of Criminal Procedure allows police officers to seize the corpus delicti and related items on their own initiative. They must then submit the verbatim report within 48 hours to the examining magistrate, who must validate it within 96 hours if the conditions are met, otherwise the measure is null and void.	San Marino applies general search and seizure powers to implement Article 19.1. Provisions specific to computer data and systems could permit greater clarity and legal certainty.

Party	Legislative and other measures	Assessment
	It was also indicated that police forces are authorized to access a computer system when delegated by the judiciary if the access credentials are lawfully acquired. In the absence of lawfully acquired access credentials, but with the authorization of the Judiciary, the Gendarmerie Corps - Operational and Judicial Police Unit may be authorized to carry out remote access to the computer system. The San Marino Court authorizes the police to conduct investigations, searches and seizures, which are carried out by or instigated by them independently regarding crimes. To analyze seized data, files and hardware, the police work with technical experts in the field under the judge.	
Senegal	Search and seizure of electronic data are governed by Articles 90-1 to 90-14 of the CPC as amended in 2016. The provisions are applicable to crimes against, or committed using, information systems. They also apply to all other types of crime whose elements of proof may be found in information systems. Per CPC Articles 90-4 through 90-6 and 90-8, searches are authorised and supervised by the Prosecutor of the Republic or by a juge d'instruction. They are executed by the juge d'instruction or by the judicial police under the supervision of the prosecutor or juge d'instruction. Searches are permissible only if the targeted data are absolutely necessary to the investigation, with strict conformance to the principle of the legality of evidence. The data must be useful for the purpose of determining the truth. The person in charge of the system must be informed about the search carried out and about the data copied, removed or rendered inaccessible. Article 90-6 addresses urgent cases in the sense that, if seizure of parts of an information system is not advisable, data that would be useful to determining the truth may be copied, including by using storage media belonging to persons authorised to use the system. It appears that Articles 90-11 and 90-9 permit the use of lawfully acquired credentials, since they authorise officials to use any appropriate technical measure to collect data relating to specific communications transmitted via an information system. Officials may also use technical processes, programs, etc, to restore deleted data or to attribute acts. Use of such measures/procedures is	Senegal applies specific search and seizure powers to implement Article 19.1.

Party	Legislative and other measures	Assessment
	permitted only when necessary to obtain the evidence and must be authorised and supervised by the prosecutor or juge d'instruction. Article 90-10 permits the competent authorities to install and use remote tools to obtain evidence useful for a case.	
Serbia	Article 19.1 searches are requested by public prosecutors, allowed or ordered by courts and executed by the police. The request and order are based on reasonable doubt that a crime has been committed (after a report of the crime or its accidental discovery). Search orders can apply to computers, systems, data and storage media. The general search and seizure powers in the CPC apply to all crimes in the Criminal Code; the special investigative powers relating to electronic searches and seizures apply only to certain crimes (specified and provided in Serbia's response). Regardless of whether the order derives from general powers or special investigative powers, electronic evidence may be searched. Specialised units within the police have the necessary expertise. The police and specialised units have adopted non-public standard operating procedures. According to Article 158 of the CPC, searches and seizures may be conducted without a court order in certain urgent circumstances (listed in Serbia's response). Serbia stated that the interaction of Article 147 of the CPC with Article 158 makes clear that electronic data and storage devices are within the categories of items that may be taken in such urgent seizures. Use of lawfully acquired credentials is permissible if they are turned over voluntarily or acquired by law enforcement when executing a court-approved measure. The CPC does not differentiate between regular and covert remote access. Either may be sought by the prosecution and approved by the court. More specifically, if the elements of Article 161 of the CPC are fulfilled, a court may order (on motion by the prosecution) "computer searches of already processed personal data and other data and their comparison with data relating to the suspect and the criminal offence."	Serbia applies a combination of general and specific search and seizure powers to implement Article 19.1.

Party	Legislative and other measures	Assessment
Sierra Leone	Search and seizure of stored computer data is provided for in Section 10 of the Sierra Leone Cybersecurity and Crime Act 2021. The authorities informed that, according to section 10 of the Sierra Leone Cybersecurity and Crime Act 202, an enforcement officer may apply to a Judge of the High Court for a warrant to authorize the access, seizure or to secure a computer system, program, data or computer data storage medium that may be required as evidence in proving an offence in a criminal investigation or criminal proceedings or has been acquired by a person as a result of the commission of an offence. There are no special rules regarding emergencies or other urgent circumstances. The legislation empowers the competent authorities to search or similarly access a computer system and data therein using lawfully acquired access credentials. The legislation does not authorize the competent authorities to search or similarly access a computer system and the data contained therein using covert remote access. The competent authority that authorizes is the judge and those who carry out a search are law enforcement agencies like the police and other competent authorities.	Sierra Leone applies specific search and seizure powers to implement Article 19.1.
Slovak Republic	Search of the computer system and data stored therein is possible under the general powers for house search (Section 99), inspection of other premises and land (Section 101) and personal search (Section 102) of the CPC. Depending on the stage of the investigation, an order must be obtained from a court or from a prosecutor. The application must show proper justification. Emergencies are not specifically regulated, but there is a 24/7 duty system for prosecutors and judges to address urgent cases.	Slovak Republic applies general search and seizure powers to implement Article 19.1. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.

Party	Legislative and other measures	Assessment
	The CPC does not provide for the use of lawfully acquired access credentials. Such credentials may be turned over voluntarily by the target or obtained based on court or prosecutor's order. Covert remote access is not authorised by the CPC. Authorising authorities are the court or the prosecutor, depending on the measure performed, the stage of the proceedings and the type of data requested. The measures are executed by forensic specialists, who have particular training and ranked qualifications.	
Slovenia	Two primary articles of the CPC, Articles 219a and 223 a, address searches and seizures of electronic data. Reasonable grounds justifying a search must exist (see below). If such bases exist, a search may be performed based on 1) the prior written consent of the relevant person or 2) a well-founded written court order based on an application developed by the prosecution and police. The execution of the search is carried out by specially-trained police. If a direct and serious danger to the safety of people or property exists and a written order cannot be obtained in a timely way, the investigating judge may orally order the search based on an oral application by the prosecutor. This action must be documented and ratified within twelve hours; otherwise, the evidence must be destroyed. Owners or users of electronic devices must provide access to the item, encryption access keys or passwords, and any necessary explanations about the functioning of the item. Persons who refuse to cooperate may be punished, including by imprisonment (except for persons in certain categories, such as defendants). Apparently, these credentials may then be used. Covert remote access is not available except in very limited circumstances relating to financial institutions.	Slovenia applies specific search and seizure powers to implement Article 19.1.
Spain	Search of the computer system or data located in computer devices or mass storage systems was explicitly regulated by the Spanish Criminal Procedure code in 2015. The reform to the Law operated by LO 13/2015 incorporated into the procedural measures Article 588 sexies (e) inspired by Article 19 of the Budapest Convention.	Spain applies specific search and seizure powers to implement Article 19.1.

Party	Legislative and other measures	Assessment
	Spain informed that In practice, search of computer devices is carried out with the knowledge of the interested party, who can give his consent for this diligence to be carried out and only in the absence of such consent will be necessary the judicial authorisation. Article 588 bis (a) LECrim provides that technological research measures, unless there is the consent of the data subject, may be agreed only by means of a *judicial decision issued in full compliance with the principles of specialty, suitability, exceptionality, necessity and proportionality of the measure*. Spanish law expressly provides in several articles of its procedural legislation for the notification of the search measure both to the accused and to third parties concerned (arts. 566, 569 and 588). Spain's legislation provides for certain exceptions in cases of emergency meaning those cases in which delaying the practice of the investigative measure may impair the obtaining of evidence under suitable conditions to be used as evidence in criminal proceedings. According to jurisprudence, if credentials are legally obtained during a home search and the judge authorises their use, there is no legal problem with using them to analyze a device. This use of credentials is considered lawful if they were obtained without violating fundamental rights. Article 588 septies (i) allows the judge to authorise a remote search of a computer, electronic device, or system without the owner´s knowledge in cases of specific crimes. The judicial decision must specify the scope and manner of access, the software to be used, the agents authorised to carry out the search and measures to preserve data integrity. Service providers and system owners must cooperate with the investigating agents, who may also order anyone with knowledge of the system to provide necessary information. The measure can't last up to three months, with liability for those who fail to cooperate. The search must be authorised by the judicial authority. Police forces of specialized units carry out the search and analysis of the device which can be done physically or by partial overturn. The technical examination is carried out on a copy-mirror of the system under analysis to prevent alteration of the original content, and the seized device is kept at the disposal of the judicial authority.	

Party	Legislative and other measures	Assessment
Sri Lanka	Searches and seizures of stored computer data are primarily governed by the Computer Crime Act No. 24 of 2007 and the Penal Code. Other statutes (specified in Sri Lanka's response) may apply. The powers deriving from the CCA are primarily related to offences against or by means of computers. They may also apply to other offences if a computer or electronic data is integral to the commission of the offence or holds evidence related to the offence. According to Section 18 of the CCA, searches and seizures in non-urgent circumstances may be authorised and conducted only pursuant to a warrant issued by a magistrate. Police officers who access computers in investigations under the CCA must be pre-certified by the Inspector General of Police as competent in digital investigations. Forensic experts may be utilised under police supervision. It appears that no procedural guidelines or standard operating procedures have been adopted, but Sections 20-24 of the Computer Crime Act detail the procedures for searches (normal use of computer not to be hampered ; power of police officer to arrest, search and seize ; police officer to record and afford access to seized data ; duty to assist investigation ; confidentiality of information obtained in the course of an investigation). Section 18/2 of the Computer Crime Act permits searches without warrant if the investigation must be conducted urgently, there is a likelihood of the evidence being lost, destroyed, modified or rendered inaccessible, and there is a need to maintain the confidentiality of the investigation. Sri Lanka does not have authority to use lawfully acquired access credentials. Sri Lankan legislation does not provide for covert remote access.	Sri Lanka applies a combination of general and specific search and seizure powers to implement Article 19.1.
Sweden	Search and seizure are covered by several general CPC rules (e.g., search of premises, body search) and by rules specific to electronic data and devices (covered remote access called secret data interceptions). There are requirements for notification and presence of the affected person or a witness. An order authorising the search of premises (which may lead to the search of electronic devices and data) is normally issued by the leader of the investigation (from the Police Authority) or a prosecutor. Which official leads the investigation, and its complexity, will determine who authorises	Sweden applies a combination of general and specific search and seizure powers to implement Article 19.1. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.

Party	Legislative and other measures	Assessment
	searches and seizures. At the stage when a person is reasonably suspected of having committed the offence, the investigation would be led by the prosecutor unless the investigation is of a less-complicated matter. The extent to which coercive measures are required will affect whether the investigation is considered sufficiently complex that it should be led by a prosecutor. If the search will be extensive or cause extraordinary inconvenience, the search should be conducted only pursuant to an order issued *by a court* unless the delay would entail risk. "If delay entails risk" means that the coercive measure would be pointless if not performed immediately. In that case, the police may search without an order. Objects found during a search that are reasonably presumed important to the investigation may be seized. Objects otherwise found may be seized pursuant to an order from the leader of the investigation or the prosecutor. If delay entails risk, objects may be seized absent an order. The execution of searches is conducted by the investigating authority, ideally in cooperation with experts in digital forensics or other specialised personnel. Especially complex cases are handled by experts at the National Forensic Centre of the Police Authority. Lawfully acquired access credentials may be used, subject to the usual requirements regarding search and seizure. Covert remote access called secret data interceptions is possible, but it may be approved only if the reasons for such access outweigh the effect on the rights of the searched person (in the case of a computer system, the searched person is normally the target). Permission for such access is requested by a prosecutor, and the court will hold a hearing with an appointed public representative. In urgent cases, a prosecutor may approve such access before the matter is heard by the court. Covert remote access is available only if the measure is of extraordinary importance in cases where there is a potential sentence of at least two years' imprisonment or in relation to a certain list of crimes. The executing authority in such cases must appoint at least one person with special expertise to conduct the measure. Sweden supplied helpful ancillary materials and information about its search and seizure law and practice.	

Party	Legislative and other measures	Assessment
Switzerland	The regulations for non-electronic searches and seizures also cover searches and seizures of electronic systems and data. In addition, the CrimPC in part explicitly provides for searches and seizures of electronic data and storage. Generally, both searches and seizures may be authorised by a written order, issued if the several elements specified in the relevant CrimPC sections have been satisfied. In principle, a prosecutor may also order a search without court authorisation. Therefore, a search does not generally require authorisation by a court. However, the searched person may request that documents in protected categories be sealed, whereas an unsealing shall be pronounced by an independent court. The execution of searches is carried out by the police and, if necessary, additional technical experts. Emergencies and urgent cases include those in which the police require immediate access to data or storage that has just been discovered, imminent danger that may occur, or a realistic danger that delay will mean that traces of the crime, object or assets will be lost. As an exception, in imminent danger cases, a search may be carried out by the police without prior written order, but the action must be reported promptly and must be confirmed by the competent criminal authority in writing. There is a distinction between seizures and securing of evidence by the police. Whether the absence of a warrant will render the evidence inadmissible is decided on a case-by-case basis. The use of lawfully acquired credentials is permissible per the jurisprudence of the Supreme Court. Remote access is available with lawfully acquired credentials, assuming that the requirements of the CrimPC are met. Additional CrimPC articles allow limited, non-content monitoring of correspondence by telecommunications within very restrictive parameters.	Switzerland applies a combination of general and specific search and seizure powers to implement Article 19.1.
Tonga	Section 9 of the Computer Crimes Act [Cap 4.02] governs electronic searches and seizures, which may be conducted (with some exceptions) only on a magistrate's issuance of a warrant. The sworn warrant application and affidavit must be supported by reasonable grounds to suspect that a computer, system, data, etc, may be material evidence of an offence or has been acquired as a result of an offence. The police execute the search and seizure (see other details infra), complying with the procedures in the section, such as inventorying what has been seized. The statute may require that the police official executing the measure hold a certain rank. There are no notification requirements.	Tonga applies a combination of general and specific search and seizure powers to implement Article 19.1.

Party	Legislative and other measures	Assessment
	There is no legislation specific to electronic searches in emergencies or other urgent circumstances. However, Section 123 of the Police Act could be used to conduct searches of data in emergencies, since it provides for warrantless searches in serious offence cases that meet several other elements of the section. National security matters or threats to life may constitute emergencies. Time-sensitive investigations or the likely destruction of evidence may constitute urgent circumstances. As further explained in Tonga's response, several other acts provide for search in emergencies and search and seizure without warrant in emergencies if certain requisites are satisfied. There is no specific legislation addressing access using lawfully acquired credentials. In practice, applications for generic warrants include requests to obtain access credentials, so such warrants cover acquisition of access credentials. This mechanism has been used for investigations under various acts. Covert monitoring powers exist within several acts, including the Police Act. More specifically, Section 14 of the Computer Crimes Act provides for interception of electronic communications if certain requirements are satisfied. Searches pursuant to Article 19.1 are authorised by a magistrate or Supreme Court judge, depending on the statute involved. Searches are executed by police officers or "authorised officers or persons" assisting the police. Such authorised persons may include CERT Tonga personnel or other forensic specialists. In conjunction with specialists, the Tongan police are developing standard operating procedures for the use of Cellebrite devices. CERT Tonga is drafting standard operating procedures addressing its collaboration with the police.	
Tunisia		
Türkiye	Electronic searches and seizures are regulated by at least two statutes. A judge orders the measure, assuming that the basis for it is sufficient. Where delay may be prejudicial, a prosecutor may order a search. The prosecutor's order must be ratified by the judge very promptly; if the time expires, or if the decision is not ratified, the collected data must be destroyed. The search or seizure is carried	Türkiye applies specific search and seizure powers to implement Article 19.1.

Party	Legislative and other measures	Assessment
	out by law enforcement units. Forensic experts may be involved or seized items may be sent to forensics experts for examination. In emergencies, the prosecutor may order a search subject to the court ratification above. Such emergencies include cases where there is a risk of loss of data, the crime under investigation carries a heavy penalty, or the suspect has been detained to prevent tampering with the evidence. It appears that the use of lawfully acquired credentials is not permitted. Covert remote access may be used in investigations of online betting. The CPC does not regulate this with regard to other offences.	
Ukraine	Ukraine applies several criminal procedural code provisions") that has some characteristics that implement Article 19 of the Convention. Art. 159 provides the possibility of temporary access to things and documents which consists in providing the party to criminal proceedings by the person in possession of such things and documents, however it is yet to be determined how the provisions extends to computer data. According to part two of Article 159 of the Criminal Procedural Code of Ukraine, temporary access to things and documents is carried out based on a ruling of the investigating magistrate or court. Examination of computer data is carried out by the investigator, prosecutor. The responses specify that in accordance with the requirements of Article 159 of the Criminal procedure Code, in a case when computer data is known, a prosecutor or investigator has the authority to exercise temporary access to electronic information systems, computer systems or parts thereof, mobile terminals of communication systems, which is carried out by taking a copy of the information contained in such electronic information systems, computer systems or parts thereof, mobile terminals of communication systems, without removing them. On the other hand, if there is not knowledge on the place of storage of the computer system or data stored , as well as a computer storage medium in which computer data can be stored, the authority in accordance with Article 234 of the Criminal Procedure Code of Ukraine is provided to conduct a search in order to identify and	It appears that Ukraine applies a combination of general and specific search and seizure powers to implement Article 19.1. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.

Party	Legislative and other measures	Assessment
	record information about the circumstances of a criminal offense, to find an instrument of a criminal offense. In urgent cases related to the preservation of human lives and property or the direct prosecution of persons suspected of committing a crime, another procedure established by law for entering a person's home or other property, conducting an inspection and search therein is possible. The procedural basis for conducting an urgent search is Part 3 of Art. 233 of the Criminal Procedure Code. According to part six of Article 234 of the Criminal Procedural Code of Ukraine, during a search, a prosecutor has the right to overcome logical protection systems if the person present during the search refuses to open them or remove (deactivate) the logical protection system or the search is carried out in the absence of persons. This rule may be interpreted as the power of search or similarly access a computer system and data therein using lawfully acquired access credentials.	
United Kingdom	Procedural powers that apply to the search and seizure of stored computer data arise from various pieces of legislation, some applicable to the whole territory of The United Kingdom (hereinafter "The UK") and some not. More specifically, the Police and Criminal Evidence Act 1984 (PACE), applicable in England and Wales, provides for general powers. A PACE search warrant can authorize the search for an electronic device or electronic data. It appears that similar general provisions are applicable in Northern Ireland through the Police and Criminal Evidence Order of 1989. There is no specific legal provision providing for search and seizure of stored computer data or cloud-based computer data or systems in Scotland. The powers providing for search and seizure of stored computer data in Scotland derive from pre-existing more general powers of search under the Criminal Procedure (Scotland) Act 1995 and the Criminal Justice Act 2016. Under the Regulation of Investigatory Powers Act 2000 (RIPA) which applies to the whole territory of the UK, authorities can require a person to disclose a key, code, password, algorithm, or other data	United Kingdom applies a combination of general and specific search and seizure powers to implement Article 19.1. Provisions specific to computer data and systems establishing a legal framework for the search and seizure of computer data and systems applicable in England, Scotland, Wales and Northern Ireland could permit greater clarity and enhance legal certainty.

Party	Legislative and other measures	Assessment
	to access protected information, defined as data that cannot be accessed or made intelligible without the key. Concerning to rules applicable in an emergency or other urgent circumstances, under the PACE, the law enforcement agencies can request access to data held by a person in an emergency, or request that the person retain the data until a PACE Schedule 1 warrant is obtained. Law enforcement agencies can use login details found during a lawful search to access electronic devices on site. Section 49 of RIPA allows the authorities to require a person to disclose a key, code, or password to a computer system. Failure to comply with a notice under section 49 is an offence under section 53 of RIPA. Competent authorities can obtain a Targeted Equipment Interference (TEI) warrant under s99(2) of the Investigatory Powers Act 2016 (IPA) to access a computer system and the data it contains using covert remote access. Equipment interference warrants authorize physical and remote interference with equipment for the purpose of obtaining communications or equipment data. A TEI warrant also gives a person lawful authority to intercept the stored communication. Orders are authorised by a magistrate's court. This procedure seems to be applicable in all countries of the UK. TEI can be issued by the Secretary of State (or Scottish Ministers), or a law enforcement chief as defined at Schedule 6 IPA. Decisions to issue an equipment interference warrant must also be approved by a Judicial Commissioner. Searches for electronic devices on premises in the United Kingdom will normally be carried out by warranted officers of one of the 43 territorial police forces in England and Wales, Police Scotland, the Police Service of Northern Ireland or the National Crime Agency. It should be noted that a special report prepared by the independent Law Commission on search warrants in England and Wales published in 2020 recommended expressly "updating law enforcement	

Party	Legislative and other measures	Assessment
	powers so that they more clearly apply to electronic devices and data and allow digital evidence to be seized and copied effectively".	
United States	The Constitution, the Federal Rules of Criminal Procedure, and statutes are the basis for search and seizure law. Normally a search warrant is required and is procured on application from an independent judge. The application must be supported by a sworn statement from law enforcement or the prosecution establishing justification for the search (see below). Searches are executed by authorised law enforcement officials. In emergencies – for example, if data are in imminent danger of destruction or if danger to life or of serious bodily injury exists – law enforcement may be able to search and seize data without a warrant. Law enforcement generally will need a warrant or consent to use lawfully acquired credentials. Covert remote access is available, typically requiring a warrant, if one of the several bases (in the Federal Rules of Criminal Procedure) for using covert remote access can be established. One of these bases is if the location of the computer to be searched "has been concealed through technological means."	The United States applies a combination of general and specific search and seizure powers to implement Article 19.1.

5 EXTENDING A SEARCH TO ANOTHER SYSTEM (ASSESSMENT OF ARTICLE 19.2)

This section assesses implementation of Article 19.2:

> Article 19 – Search and seizure of stored computer data
>
> 2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.

5.1 Implementation of Article 19.2: overview

5.1.1 Legislative and other measures, procedure for extending a search – summary

The Convention does not prescribe how an extension of a search is to be permitted or undertaken and this is left to domestic law. Parties have thus taken various approaches.

Numerous Parties[43] have implemented the measure through specific provisions in their domestic law.

Many States[44] require a court to authorise this measure.

Generally, when extending a search, most of the States[45] use the same procedure, as in relation to other searches. One Party (Cabo Verde) also specified that it has not yet applied the measure of extension of search.

On the other hand, for example, Sweden relies on general powers to implement Art. 19.1. It implements extension of searches through a specific power, entitled "remote search," that enables searching for data stored in a readable information system outside the electronic communications equipment used to perform the search.

The assessment of Article 19.2 focuses solely on the question whether a Party has developed the power of extension of search for purely domestic situations, i.e. when the initial computer system and a connected computer system are in that Party's territory. Whether a party may extend the search to computer systems outside its territory does not affect the assessment of

---

[43] Albania, Australia, Belgium, Cabo Verde, Canada, Croatia, Fiji, France, Germany, Greece, Hungary, Israel, Japan, Latvia, Montenegro, Netherlands, Norway, North Macedonia, Portugal, Romania, Senegal, Sierra Leone, Slovenia, Spain, Sweden, Türkiye, USA.

[44] Albania, Andorra, Armenia, Belgium, Bosnia and Herzegovina, Brazil, Bulgaria, Canada, Costa Rica, Croatia, Cyprus, Czech Republic, Denmark, Estonia, France, Georgia, Germany, Ghana, Iceland, Israel, Japan, Latvia, Liechtenstein, Lithuania, Montenegro, Netherlands, Nigeria, Norway, North Macedonia, Paraguay, Peru, Philippines, Romania, San Marino, Senegal, Serbia, Slovak Republic, Slovenia, Spain, Türkiye, United Kingdom, USA.

[45] Albania, Andorra, Australia, Austria, Belgium, Bosnia and Herzegovina, Brazil, Bulgaria, Cabo Verde, Canada, Costa Rica, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Greece, Hungary, Iceland, Japan, Latvia, Liechtenstein, Lithuania, Montenegro, Netherlands, Nigeria, Norway, Panama, Peru, Paraguay, Portugal, Romania, Senegal, Slovak Republic, Slovenia, Türkiye, USA.

its Article 19.2 implementation. Such assessment concerns exclusively measures that a Party is required to take at the national level "in its territory".

Article 19.2 does not address transborder search and seizure, whereby States could directly search and seize data stored in the territory of other States without having to go through the usual channels of mutual legal assistance. The fact that Article 19.2 does not address the issue is however without prejudice to situations where a Party may expeditiously extend the search or similar accessing to another computer system under certain conditions in other Parties' territories, as is the case of several States (Andorra, Austria, Belgium, Brazil, Estonia, Iceland, Netherlands, Portugal, Senegal, Spain). Information on such measures is included also in the following sections of this chapter, as it remains of interest to the T-CY.

In accordance with Article 39, paragraph 3, nothing in the Convention requires or invites a Party to establish powers or procedures other than those contained in this Convention, nor precludes a Party from doing so. Because the Convention is silent on this issue, it would not protect a Party who chose to access computer systems in other Parties' territories from legal liability under the laws of the Party in which the accessed computer system may be located.

5.1.2 Grounds to believe that data sought is stored in another system in its territory

When establishing grounds to believe that data sought is stored in another computer system or part of it in their territory, Parties either rely on rules established under their general legal framework (such as Czech Republic or Norway), text specifically covering search and seizure of computer data (Australia), guidelines that implement the rules that are set by the domestic law of the Parties (Bosnia and Herzegovina), or other standard operating procedures (Netherlands).

Many Parties do not necessarily define "grounds to believe" or "reasonable grounds", but their domestic law enumerates conditions that must be met to authorise an extension of searches. For example, Belgium requires that the extension must be necessary to establish the truth about the offence that is the subject of the investigation. In addition, there must be no other less intrusive measures available that can achieve the same result or there must be a risk that, without this extension, evidence will be lost. Taking other measures (e.g., several search warrants) would be thus disproportionate.

Several Parties also indicated that these grounds are determined based on the specific circumstances in the individual cases.

The following are other examples of elements of grounds to believe (or alternatives) that were mentioned in the country replies:

- Analysing and reviewing the settings on the device containing the relevant data (Austria).
- Location of the computer system (Bosnia and Herzegovina).
- "Sufficient or positive probability" that data are in the place where they are indicated (Costa Rica).
- Establishing existence of data and, if possible, location of other connected devices (Croatia).

- Reasonable suspicion that the item or person important for criminal proceedings is located in the apartment or other premises used for accommodation or belonging to the person (Czech Republic).

- Search can lead to the discovery of a document or data to be seized or copied (Finland).

- Data of interest to the investigation, objects, documents and computer data useful in establishing the truth (France).

- Imminent loss of data, existence of initial suspicion (Germany).

- Reasonable suspicion that data are stored in another computer system and data are deemed relevant for the investigation (Hungary).

- Facts indicating the likelihood that reasons for search exist (Montenegro).

- Situations where it is considered more likely than not that the accused has committed the criminal offence in question (Norway).

- Initial suspicion that a punishable act has been committed that may constitute a crime (Peru).

- Information on the basis of which the authorities can reasonably assume that the wanted objects are in the given premises or that a suspect is present there (Poland).

- "Indications" that evidence is in a reserved place or not freely accessible to the public (Portugal).

- Demonstration that sought data were found in another computer system and they were accessible from the initial system (Portugal).

- A totality of elements or facts indicating that it is likely that stored data in a system beyond the initial system could contribute to determining the truth (Senegal).

- Probability that the electronic device contains electronic data or traces of a criminal act can be discovered that are relevant to criminal proceedings (Slovenia).

- "Founded reasons to consider" - rational indications that a second system in which data relevant to the investigation are housed (Spain).

- Search may be extended in the following cases: a) in a readable information system that the person who is reasonably suspected of the offence is likely to have used; or b) the authorities may conduct a search if there is extraordinary reason to assume that information of potential importance can be found (Sweden)

- Presumption of relevance to seizure and sufficient suspicion. This is established on the basis of concrete evidence (Switzerland).

- Basis for believing the devices or data to be searched are located within the relevant district (USA)

Examples of practices include:

- Australia: reasonable grounds

Division 4 of Chapter 2 of the SD Act establishes that in order to apply for a computer access warrant, a law enforcement officer must suspect on reasonable grounds that:

- one or more relevant offences have been, are being, are about to be, or are likely to be, committed; and
- an investigation into those offences is being, will be, or is likely to be, conducted; and
- access to data held in a computer (the target computer) is necessary, in the course of that investigation, for the purpose of enabling evidence to be obtained of:
  - the commission of those offences; or
  - the identity or location of the offenders.

- Liechtenstein: means to establish grounds to believe

  Competent authorities typically establish they have "grounds to believe" that the data sought are stored in another computer system or part of its territory through the following:

  - 1. Police interviews with suspects or witnesses.
  - 2. IP addresses show different location data.
  - 3. Monitors or docking station are without a computer or notebook.
  - 4. Any other references in the computer system to external systems, that are not present.

5.1.3 "In its territory" and beyond

Like all articles in Section 2 of the Convention, Article 19.2 concerns only measures that are required to be taken at the national level. Although an extension of searches to a different territory is a measure that goes beyond of the scope of this assessment, this aspect has been of interest to the T-CY for many years.[46] Therefore, information on the application of this power beyond "its territory" is also provided in various parts of this report.

The domestic laws of some Parties impose an affirmative requirement that the connected system be in the territory of the State executing the measure (Armenia, Bosnia and Herzegovina (including entity of Federation of Bosnia and Herzegovina), Bulgaria, Costa Rica, Latvia, Paraguay, USA[47]).

More specifically, Costa Rica understands territory as a physical place (sea, air, ground territory, etc) in which it exercises its sovereign powers. It requires that the computer system where the data are stored must be in its territory, or that the provider of the service has an open business office in Costa Rica. Paraguay referred to its requirement of the implication of

[46] See the work of the T-CY on transborder access to data, on cloud evidence, or on undercover investigations and extension of searches. https://www.coe.int/en/web/cybercrime/tcy

[47] The law of United States of America (Rule 41) incorporates geographic limitations on the circumstances in which a court may authorise a search warrant. The most common basis for seeking a warrant is the situation where the property to be searched or seized is located in the district of the issuing judge, which will in all circumstances be in the territory of the United States. Rule 41 does authorise federal judges to issue warrants to authorise law enforcement to remotely access electronic storage media in the United States and seize electronically stored information, regardless of whether the media or information is in the judge's district, in two circumstances that occur in cybercrime investigations. The first, applicable here, is when the location of the media or information to be searched "has been concealed through technological means."

the element of territorial jurisdiction in the process and to that the place of the event must be stated. The domestic law of the US incorporates geographic limitations on the circumstances in which a court may authorise a search warrant.

The domestic law of other Parties[48] does not impose an affirmative requirement that the connected system be in the territory of the Party executing the measure.

This aspect of the assessment relates only to a Party's ability to extend searches within its own physical territory, i.e., when the initial computer system and a connected computer system are in that Party's territory. However, many States may extend the measure to access data possibly located abroad.[49] They indicated that the following conditions ordinarily must be met in order to search data that might be stored outside of their territory:

- Albania: necessary to specify possible location of the data, in order for the court to authorise the measure.
- Andorra: connection point such as an Andorran mailbox, a cloud connected to the system or an e-mail address, etc.
- Australia: access agreed to by an appropriate consenting official of the foreign country.
- Belgium: the authorities must carry out acts from the territory of Belgium, notification of State concerned.
- Bosnia and Herzegovina (Republika Srpska): if access from the computer system of a suspect is enabled, computer systems that can be accessed may be searched even if located in another country.
- Brazil: the fact that data may be stored abroad is not an issue when accessing the cloud, as long as the stored data is legally reachable from the Brazilian territory.
- Croatia: measure applies to computer and devices connected with the computer.
- Czech Republic: device from which the data are available must be located in its territory; the data may be located in the territory of a foreign country.
- Denmark: applies to data that may be accessed from the person's computer (even if the digital messages have not yet been technically obtained from the internet provider).
- Estonia: no limitations.
- Fiji: the powers apply to data found or accessible from Fiji.
- Finland: the powers apply to the data likely to be located within the geographical borders of Finland. Sometimes case-by-case basis considered in cases where the data can be accessed (not necessarily stored) in Finland.

[48] Albania, Andorra, Australia, Austria, Belgium, Bosnia and Herzegovina (applicable to entity of Republika Srpska and Brcko District), Brazil, Croatia, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Hungary, Germany, Iceland, Israel, Italy, Japan, Latvia, Liechtenstein, Lithuania, Montenegro, Netherlands, Nigeria, Norway, Peru, Poland, Portugal, Senegal, Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Türkiye.

[49] See also the following section on loss of knowledge of location.

- France: in case of a cloud - if the computer equipment allows a connection to a remote service, the investigators will in principle be able to access it. If data stored abroad, authorities use Article 32 of the Convention on Cybercrime.

- Georgia: access must be carried out from its territory and must be lawful (was (including by using applications that were logged in during searches).

- Germany: in cases of cloud computing when it cannot be determined where the data are located.

- Hungary: computer system from which the data is accessed must be located in its territory.

- Liechtenstein: when access to a remote computer system (e.g. service in a cloud) is available from its territory.

- Luxembourg: All data stored or accessible in/from the Luxembourgish territory may be accessed and searched.

- Malta: any act is committed outside Malta which would have constituted an offence had it been committed in Malta. if the commission affects any computer, software, data or supporting documentation which is situated in Malta or is in any way linked or connected to a computer in Malta.

- Norway: measure commenced on a Norwegian soil against a Norwegian citizen/company a Norwegian company with offices in Norway; data must be freely retrieved from the storage place abroad, remain on the foreign server, and no changes must be made to the information.[50]

- Philippines: Any part of the computer system used must be within the Philippine jurisdiction, including its interior and maritime zone.

- Poland: it cannot be established where the data are stored.

- Portugal: a search may be extended, regardless of the location of the remote system.

- Senegal: subject to applicable international arrangements, a judge may collect stored data in a system located outside Senegalese territory, assuming that the system is accessible from an initially-searched system. Such extension must be necessary to determining the truth or there must be risks of loss of evidence. The extension must reach only those systems to which persons authorised to use the initial system have access. The judge must inform the person in charge of the system unless their identity or address cannot be found.

- Spain: what is decisive is not the physical location of the data, but from where it is accessible.

- Switzerland: if the access credentials are acquired lawfully and the conditions for a search are met, a remote access is generally possible if conducted from Switzerland.

- Türkiye: the computer system "used by the suspect" in Turkish territory has a connection with the system "used by the suspect" in another country.

[50] See Appendix, The Supreme Court of Norway - Order - HR-2019-610-A (Tidal case).

- United Kingdom: warrants under IPA have extraterritorial effect. For TEI this is covered in sections 126 and 127 of the IPA.

- USA: location of the media or information to be searched "has been concealed through technological means".

Other Parties[51] stated that this aspect is not addressed in their domestic laws or that they proceed based on specific circumstances of the individual case.

Although there is no affirmative requirement that a connected system must be located in the territories of Chile, Peru, San Marino, Sierra Leone and Slovak Republic, these Parties pointed out that the territorial applicability of their domestic legislation is limited to their soil and specified that in relation to data located abroad, other available mechanisms under international law, such as MLA, must be applied.

Canada stated that its law is circumscribed by the principle of territoriality and extraterritorial extension of a search would be permissible only after enactment of a law that explicitly permitted such extensions. Grenada, The Republic of Moldova and Tonga indicated that searches/seizures are restricted only to data or systems physically within their territory.

5.1.4 Loss of (knowledge of) location / "unknown location"

Cloud computing has meant that criminal justice authorities more often face challenges where the location of the data is not known or locating data is not feasible.[52] Sometimes even the service provider might not know the exact location of data. Bearing in mind the importance of an effective criminal justice response in the face of increasing difficulties in obtaining evidence in "loss of (knowledge of) location" cases, learning how a Party approaches these situations may be beneficial for others.

In general, Parties emphasized that they first make every reasonable effort to learn the location of the data. Parties also emphasized that they use international cooperation mechanisms whenever possible. A few States did not explain how they proceed when these processes fail or cannot be used. However, most responding Parties stated that, if they had no other choice, they would knowingly extend a search to another country *under certain circumstances.* Those circumstances may be very limited. The section below details States' approaches to these issues.

In cases of loss of (knowledge of) location situations, numerous Parties[53] continue as if the data were in their territory.

However, some of the Parties specified the following elements that must be met:

---

[51] Iceland, Israel, Japan, Lithuania, Montenegro, Morocco, Slovenia.

[52] See for example Cybercrime Convention Committee (T-CY), Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY Final report of the T-CY Cloud Evidence Group, 16 September 2016. See also Sansom, Gareth (2008) about the problem of "location" in cyberspace.
http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/TCY/Gareth%20Samson%20Website%20Location.pdf

[53] Australia, Austria, Bosnia and Herzegovina, Canada, Croatia, Czech Republic, Denmark, Estonia, France, Germany, Hungary, Malta, Netherlands, Poland, Portugal, Senegal, Slovenia, Spain, Sweden, Switzerland, Türkiye.

- Australia: the person executing a computer access warrant is physically present in Australia. In addition to the location where the data is held is unknown or cannot reasonably be determined.

- Canada: the location of the data is not known, for example, in certain dark web scenarios or when a computer system has established encrypted tunnels to data storage devices in unknown locations.

- Czech Republic: possible to seize and search data available from device located in the Czech Republic.

- Denmark: if the crime subject to Danish right of punishment, investigated by Danish authorities, crime has an effect in Denmark.

- Fiji: if permitted technically by the search warrant, the data may be seized, but if any other technical methods are to be used, then another search warrant must be requested until all technical avenues are exhausted.

- France: what is decisive is from where the authorities have access and not location of the data.

- Germany: the measure may be used only when it cannot be determined where the data are located.

- Hungary: an information system through which the data are accessible must be in Hungary.

- Mauritius: Mauritian approach depends on the type of data sought and its possible location. "If it is in some domain, there is a chance of retrieving the data provided it is accessible from Mauritius."

- Netherlands: reasonable action to establish a location is taken, actions should be proportional.

- Spain: what is decisive is from where the data are accessible.

- Sweden: the measure is taken within a Swedish criminal investigation and as a consequence relates to a suspicion of a crime that falls within Swedish jurisdiction; the measure is taken with the use of equipment that is located in Sweden; the measure is taken in a manner so that the wanted information is not deleted or in another way affected in relation to its content.

- Switzerland: what is decisive is from where the data are accessed.

- Türkiye: the computer system "used by the suspect" in Turkish territory has a connection with the system "used by the suspect" in another country.

- USA: location of the media or information to be searched "has been concealed through technological means".

A few States (Chile, Costa Rica, Paraguay) indicated that in such cases they do not pursue the data if the location cannot be determined. Parties use various means to determine such data.

More specifically, Costa Rica stated that it tries to find out the seat of the provider to identify the country concerned. If the location cannot be determined, the case is dismissed. Paraguay

pointed out that it applies the principle of in dubio pro reo and dismisses the case. Grenada stated that if the location cannot be determined after all means of obtaining this information have been used, the process is stopped.

There are a number of States (Andorra, Belgium, Bulgaria, Finland, Israel, Japan, Latvia, Norway, United Kingdom, USA) that proceed on a case-by-case basis and execution of the measure depends on several elements. One Party (Dominican Republic) stated that in cases where the exact location of the data is unknown, a preservation request is made to the service provider, who will indicate the location of the stored data. Other Party (Sierra Leone) informed that so far, it has not encountered any situations when it could not be determined where the data sought is stored.

Some of those States indicated the following elements which are taken into account by authorities when they exercise the powers:

- Belgium: Access from Belgium, (notification not required, as the state concerned is not known).

- Bulgaria: tries to determine location of remote data by using all possible means, further steps depend on decision of the authority pursuing the data.

- Japan: Article 32 of the Convention on Cybercrime is followed, there is lawful and voluntary consent of a person with lawful authority to disclose the records. Such approach confirmed also by a judicial precedent.

- Norway: tries to get information from other States, EUROPOL, CERTs. When possible, to obtain consent, Article 32 of the Convention on Cybercrime is used.

A few States indicated that the issue is not addressed in their domestic law (Georgia) or that they use operational procedures to determine the location of the data (Panama, Slovak Republic) without further specifying how they proceed if the location of the data cannot be determined.

Examples of practices include:

- Bosnia and Herzegovina: steps to identification of the data

  The authorities must first attempt to identify the location of the data sought through the use of all available means, such as IP address tracing, network mapping, and other technical methods. If the authorities are unable to determine the location of the data using these methods, they must then submit a request to the court for a warrant to search and seize the data from any computer system that may reasonably contain data sought.

- Finland: what to consider when measure is pursued

  In each individual case, authorities aim to establish the location of the data with all available means. If not established, the following points, among others, are considered depending on the case:

  - the nature of the offence under investigation and any internationally binding bilateral and multilateral agreements;
  - compliance with the due diligence principle and related obligations;
  - the suspect's nationality and country of permanent residence;

- the place of commission of the offence, any links to another State, the place where damage occurred, and the location of any victims and witnesses;
- the impact of the measure and procedures on the sovereignty of the other State;
- the impact of the measure and procedures on the target persons;
- the measure will not interfere in the internal affairs of the other State in any respect, or target any information or services that are necessary for carrying the essential duties of the other State;
- the measure will not cause any material damage or delete or edit data or cause malfunction of the target devices;
- legal remedies available to the target persons.

5.2 Implementation of Article 19.2 – Assessment

Answers to the following questions of the questionnaire were assessed:

- 2.2.1 Please summarise what legislative or other measures have you undertaken to ensure that your authorities are able to extend the search as described in Article 19.2.
- 2.2.2 Please summarise the procedure (including authorisations required and investigative techniques applied) for extending a search or similar accessing to another system in practice.
- 2.2.3 Please summarise how your legal framework applies the "grounds to believe" element of Article 19.2, including how competent authorities typically establish that they have "grounds to believe" that the data sought is stored in another computer system or part of it in its territory.
- 2.2.4 Please summarise how your legal framework applies the "in its territory" element of Article 19.2, including whether or not your framework imposes an affirmative requirement that the connected system be in your territory.54
- 2.2.5 How do you proceed in cases when it cannot be determined where the data sought is stored ("loss of (knowledge of) location situations")?

Party	Legislative and other measures	Assessment
Albania	Albania indicated that the specific powers of extension of registration are provided for in Article 208/A, paragraph 2 of the CPC. The procedure is the same as for the seizure of a computer system in the territory - the court authorises the prosecutor at his request, and then the prosecutor or the judicial police officer carries out the search and seizure. The prosecutor may also appoint an expert if necessary. The investigation techniques depend on the specifics of the situation and the type of computer data required. Regarding how the authorities apply the "grounds to believe", Albania indicated that Article 208/a of the CPC states that it's the court that decides whether there are reasonable grounds to believe that the computer data is stored in another computer system. There is no definition of reasonable grounds, and it is often decided on a case-by-case basis.	Albania applies specific search and seizure powers to implement Article 19.2.

[54] See the discussion in paragraphs 192 and 193 of the Explanatory Report.

Party	Legislative and other measures	Assessment
	Regarding how authorities apply the term "in its territory", Albania indicated that Article 208/a of the CPC does not specify the location of the initial computer system, nor the location of the computer system connected to the initial computer system. So, there is no procedural requirement related to the location of the computer system, if it is lawfully accessible from the original computer system. There is no procedural provision for the case where it is not possible to determine where the data sought are stored, "loss of knowledge of location situations", but in the interpretation of Article 208/A of the CPC, it is necessary to specify the possible location of the data and the computer system for the court to authorise the search and seizure. Alternatively, Art. 32 of the BC may be used to seize publicly available data with an undetermined location.	
Andorra	No specific legislation exists addressing Art. 19.2. The previously-described search procedures and investigative techniques are applicable here also. Judges may authorise such extensions, for example to a part of the cloud that is linked to the initially-searched system. Grounds to believe are established in any number of usual ways – for example, via information from a third party or evidence derived from the initial search. Information systems may be searched only if they are in the territory of Andorra. However, data outside Andorran territory may be searched if they are connected in some way to a system located in the country – for example, by an email address or a linked part of the cloud. If the location of data cannot be determined, Andorra takes a case-by-case approach.	Andorra applies general search and seizure powers to implement Article 19.2. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.
Argentina	The CPC at the federal level does not have a specific rule regarding 19.2, but the procedural power is implemented through general powers and accepted practices. Argentina has reported that some of the provincial legislations, such as those of Salta and Mendoza, provide for specific regulations.	Argentina applies general search and seizure powers to implement Article 19.2. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.
Armenia	Armenia stated that it has implemented legislative and other measures to enable the extension of searches, as in Article 19.2, when there are grounds to believe that the data is within the territory and if the data is	Although it appears that Armenia applies specific search and seizure powers to implement Article

Party	Legislative and other measures	Assessment
	lawfully accessible from or available to the initial system. Armenia mentions Article 236 as the relevant legal basis for the implementation of Art. 19.2. However, it is not clear how this provision addresses requirements of Art. 19.2. Typically, the authorities will seek judicial authorisation (on the grounds above) to extend the search. If the extended search is authorised, various investigative techniques may be used, including requesting cooperation from an owner or administrator, issuing subpoenas or warrants, or using technical means to access and retrieve the data. "Grounds to believe" is interpreted as reasonable grounds indicating that the data sought is stored within Armenia's territory. To establish this, authorities typically rely on investigative information, intelligence or evidence, which may include information obtained during an initial search, information from informants, technical analysis or other factors. Under the legal framework, the "in its territory" element requires that the data is believed to be stored within Armenian territory, along with an affirmative requirement that the connected system be located within the territorial jurisdiction. The authorities in Armenia cannot proceed in cases when the location of the data cannot be determined. Knowledge of the location of the data is a mandatory requirement (as like in the case of traditional search where the exact address is required).	19.2., it is not clear how Art. 236 addresses the requirements of Art. 19.2. of the BC. More specific provisions could permit greater clarity and enhance legal certainty.
Australia	Several sections of the Crimes Act and SD Act permit law enforcement at the searched premises to access data remotely. These searches must be conducted pursuant to the procedures described above. Australia uses a standard of suspicion of "reasonable grounds that the data constitutes evidential material." The Australian statutes do not explicitly impose an affirmative requirement that the connected system be in Australia. A warrant may be issued permitting the search of a person whose location cannot be predicted; remote access does not depend on the location of the data. The SD Act envisions extraterritorial searches under certain circumstances with the permission of the relevant foreign sovereign in conjunction with a proper Australian warrant.	Australia applies a combination of general and specific search and seizure powers to implement Art. 19.2.

Party	Legislative and other measures	Assessment
Austria	The power to seize data from a storage medium includes data accessible from, but not stored on, that medium. The order must extend the seizure to other media and systems. This procedure applies when there are grounds to believe that the other media or systems are outside Austria; the legal framework does not impose an affirmative requirement that they be within Austria. Similarly, loss of knowledge of the location of data does not prevent a seizure. The grounds to believe element is established based on the circumstances of the case.	Austria applies specific search and seizure powers to implement Article 19.2.
Azerbaijan	There are no specific provisions regarding the extension of searches per Article 19.2, but the general provisions for searches and seizures apply. Law enforcement or investigative authorities must present evidence and justification to a court to demonstrate the necessity and relevance of the extension. Such presentations often include specifics about the investigation, the relevance of the data sought, and the potential connection between the initial and second systems. If the evidence justifies it, a judicial authority will issue an order for the extension, outlining the scope of the extension and naming the systems to be accessed and the deadline for the search. Law enforcement or investigative agencies then execute the access within the parameters of the order. "Grounds to believe" is implemented as "sufficient reason," per Article 242.1 of the CPC, to believe that items may be of evidentiary importance and be at certain places or with certain persons. This is shown by presenting evidence and information obtained through investigation, including metadata, communications records, or digital surveillance or monitoring. Application can then be made for an order extending a search. "In its territory" is applied via Article 3 of the CPC, which provides that the CPC is applicable throughout the territory of the republic without limitation unless other articles of the code create exceptions. The CPC does not explicitly impose an affirmative requirement that a connected system must be within the territory. The application of rules governing the territorial scope of criminal procedure legislation is determined by international agreements to which Azerbaijan is a signatory. Thus, while the default application is to remain within the territory, it is suggested that the legal framework allows for flexibility in addressing cross-border aspects of investigations, potentially accommodating scenarios in which the connected system is physically outside territorial borders but within the scope of the agreements.	Azerbaijan applies general search and seizure powers to implement Article 19.2. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.

Party	Legislative and other measures	Assessment
	Azerbaijan makes extensive efforts to locate data if its location is unclear (see responses). It did not indicate its approach when the location of the data cannot be determined.	
Belgium	Articles 88ter and 39bis together provide that a juge d'instruction may order the extension of a search in an information system to a connected system (to the extent accessible to normally-authorised users), even if the second system is in a different place or beyond Belgian territory. These articles specify the required procedures and preconditions, including that no investigative method other than the extension of the search will be adequate. Should it become clear that searched data are outside Belgium, whether or not its location is identifiable, the data are merely copied, not rendered inaccessible. The relevant foreign state is then notified if known. These procedures must be authorised by a juge d'instruction. "Grounds to believe" is not defined in statute but the prerequisites for action are in the statutes, as described previously. The Belgian system does not impose a *requirement* that a system be situated on Belgian territory. Rather, it presumes that investigations should be confined to national territory except to the extent that, as described, Belgium has legislated a "cautious but pragmatic" approach to extraterritoriality.	Belgium applies specific search and seizure powers to implement Article 19.2.
Bénin	Article 587/1 of the digital code act provides specifically for the extension of searches to a second system that is available to the first. In practice, the juge d'instruction issues the appropriate order and it is executed by an investigative unit of the police, to which a tech expert may be attached. "Reason to believe" as in Article 19.2 is based on concrete, reasonable indications that justify the issuance of a search order by a juge d'instruction or prosecutor. Article 587 of the digital code law expressly covers data stored on Beninese territory that are useful for the establishment of the truth. As noted above, the article provides for the search of systems or storage media available to the first system. "In its territory" is understood to mean either that a system is located partially or totally in Beninese territory or a system is located partially or totally outside Beninese territory but is available from within Beninese territory.	Bénin applies specific search and seizure powers to implement Article 19.2.

Party	Legislative and other measures	Assessment
	Article 587/2 specifies that, if the authorities are aware beforehand that a system is outside national territory, the juge d'instruction will obtain the data by letter rogatory. When the location of data cannot be determined but is stored in a cloud or another external service, the authorities may approach the target's service provider with any available information to seek the provider's cooperation. In cases in which the available information allows access to the data without the need to geolocate it beforehand, the authorities may proceed with access and determine the location later if the evidence is indispensable.	
Bosnia and Herzegovina	Bosnia and Herzegovina has no specific legislative or other measures regarding extensions of searches as in Article 19.2. After an initial search of properly-seized devices, investigators may determine that part of a connected system is in a location different from the searched location. In that case, a second warrant will be obtained if the data are expected to be in the country. Otherwise mutual legal assistance will be used. In the codes of Bosnia and Herzegovina, the Federation Bosnia and Herzegovina, and Brcko District, the procedures for extending a search follow the usual rules described above. The Republika Srpska CPC does not contain any particular provisions referring to extension of search to connected systems. The grounds for this are in the law's definition of "computer system," which is defined as any device or a set of mutually connected or related (electronic) devices. Therefore there are no particular requirements. The normal processes are followed. If there are sufficient grounds to believe that the connected system is involved with the commission of a criminal offence, a new court order may be procured. In Bosnia and Herzegovina and the Federation Bosnia and Herzegovina, "grounds to believe" are interpreted generally in the same way – that is, the warrant application in each case must include concrete facts (such as the type of data sought) tending to indicate that the desired data will be found in the system to be searched. The standard in Republika Srpska has a higher degree of exigence. Instead of "grounds to believe", to allow the extension of the search, the law requires "sufficient grounds for suspicion" that the data are located remotely.	Bosnia and Herzegovina applies general search and seizure powers to implement Article 19.2. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.

Party	Legislative and other measures	Assessment
	Bosnia and Herzegovina and Federation Bosnia and Herzegovina authorities may extend a search only if the data are believed to be within the territory. In Brcko District, the law does not clarify if these territorial limits operate; in Republika Srpska, there are no legal restrictions regarding territorial limits. That is, in Republika Srpska systems in another country may be searched if they are related to, and can be reached from, an initial system that is searched pursuant to proper procedure. Not all the four codes in force in the country consider specifically the cases of "loss of knowledge" of location". The code Bosnia and Herzegovina allows authorities do conduct a search of data whose location is unknown, but only after demonstrating to a court a detailed and rigorous attempt to determine the location. In these cases, the usual legal procedures must be followed. Regarding the code of the Brcko District, respecting this type of searches, it disregards the location of the data focusing on the location of the owner or controller of the data.	
Brazil	Although the measure described in Article 19(2) is not provided for in Brazilian legislation, the authorities may extend a search or similar access to another computer system or part thereof if they have grounds to believe that the data sought are stored in another system or part thereof within their territory and such data are lawfully accessible from or available to the original system. The extension of the search must be authorised by a court order or a search warrant and must comply with the specific requirements and procedures established by Brazilian law, based on ordinary Article 240 for a general search and seizure. Even if it is not expressly provided for in an article of the criminal procedure code, it has been accepted by jurisprudence. In practice, extending a search or similar access to another system in Brazil requires a court order or warrant, based on reasonable suspicion of the commission of an offence, specifying the location of the search, the type of data or information to be accessed and the time frame for the search. The authorities may use computer forensic techniques to locate and access the relevant data or information on the other system or use undercover operations or confidential informants to gather information about the other system or the data or information sought. "Grounds to believe means" that there are enough elements to support this statement.	Brazil applies general search and seizure powers to implement Article 19.2. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.

Party	Legislative and other measures	Assessment
	The "in its territory" is applied in a way that generally requires the connected system to be located in Brazil. Brazilian law does not impose an affirmative requirement that the connected system be in Brazil, but the authorities must have jurisdiction over the system or data sought to lawfully extend the search or similar access to it. Brazilian law recognizes jurisdiction over computer data stored or accessible within its territory, regardless of whether the computer system itself is physically located in Brazil. Therefore, if the authorities have 'reasonable grounds' to believe that the data sought are stored in another computer system or part thereof in Brazil, and that the data are lawfully accessible from or available to the original system, they may extend the search or similar access to that system, even if it is physically located in another jurisdiction. In cases where the Brazilian authorities cannot determine where the requested data are stored, or where the location of the data is unknown, they may use various investigative techniques to try to locate the data as using technical expertise to conduct a thorough analysis of the computer system(s) in question to try to locate the data sought. This may include the use of data recovery tools, analysis of system logs, examination of metadata and other techniques. In a search and seizure that requires accessing the cloud, the fact that it may be stored abroad is not an issue as long as the stored data is reachable from the Brazilian territory and there's a judicial authorisation granted. If it is known that the computer systems or data sought are located outside Brazil, mutual legal assistance mechanisms may be used to request assistance from foreign authorities to locate the data.	
Bulgaria	No specific legislation has been adopted. Although extensions of searches are usually conducted without a prior authorisation, they must be approved by the court within 24 hours. In such a case, the presence of relevant computer data on another information system will be described in the protocol created during the initial search. Typically, the computer expert or the police officer who is present on the spot of the initial search would state that there are "grounds to believe" that in another location there is computer data relevant to the case.	It appears that Bulgaria extends searches based on provisions applicable to authorise search.

Party	Legislative and other measures	Assessment
	If it is discovered that the data are stored abroad, other international cooperation measures are taken, namely expedited preservation of data in accordance with the Budapest Convention. Efforts are made to collect as much evidence as possible to determine where the data are stored. Authorities proceed on a case-by-case basis. The applicable provisions are mentioned under 4.2.	
Cabo Verde	Cabo Verde has informed that its CL allows for the extension of a search to another computer system, or a different part of the system being searched, provided that the data is legitimately accessible from the initial system. This extension requires authorization or an order from the competent authority, by paragraphs 1 and 2 of article 17, No. 5. If it becomes necessary to produce evidence during the process to discover the truth, the competent judicial authority may authorize or order a search of a specific computer system to obtain specific and determined computer data. Whenever possible, the authority should preside over the due diligence. The order has a maximum validity period of 30 days, under penalty of nullity. According to Cape Verdean legislation, the extension of a search regime is the same as that for an initial authorization. In summary, if a search authorized by a judicial authority needs to be extended to another system, the interested party must demonstrate that access to the other system is possible from the initial one and request authorization from the competent judicial authority to carry out the search. The request should specify the system or part of it to be searched. Cabo Verde has stated that their norm does not apply the element 'in its territory'. Instead, it refers to the data being sought in another computer system or a different part of the system being searched. The law also does not explicitly demand a positive requirement that the connected system be within its territory. However, this norm has not yet been applied in specific cases. Cabo Verde stated that existing legislation does not cover the cases when it cannot be determined where the data sought is stored ("loss of (knowledge of) location situations").	Cabo Verde applies specific search and seizure powers to implement Article 19.2.

Party	Legislative and other measures	Assessment
Cameroon	The law does not yet include provisions for extending searches as in Article 19.2. "Grounds to believe" and "in its territory" are therefore not specified (in this context).	Cameroon is not yet in line with Article 19.2.
Canada	Per subsection 487(2.1) of the Criminal Code, a search may be extended to data that is available to the initially-searched computer system. The procedures are as described above. "Grounds to believe" is implemented as reasonable and probable grounds to believe that an offence has been committed and that there is evidence to be found at the place to be searched. There is an extensive caselaw on the type of evidence that may be used to justify the issuance of warrants as well as the consequences of defective or inappropriate warrant applications. The ambit of Canadian law is circumscribed by the principle of territoriality. Extraterritorial extension of a search would be permissible only after enactment of a law that explicitly permitted such extensions. When the location of data cannot be determined, it may be possible to obtain a general warrant. If that warrant authorises the search of data that is "available to" a system, "arguably, the territorial ambit of the search power may be unknowingly extended outside of the territory in question."	Canada applies a combination of general and specific search and seizure powers to implement Article 19.2.
Chile	There is no specific power in the domestic law of Chile that would provide for this measure. The search can be extended if it has judicial authorization. In practice, to extend a search or to obtain similar access to another system, the procedure requires a judicial authorisation. Article 12 of Law 21,459 provides for the existence of reasonable suspicion, based on specific facts, that a person has committed or is about to commit any of the offences referred to in Articles 1, 2, 3, 4, 5 and 7 of the law. All the mentioned rules apply to all crimes committed within the territory according to the general rules.	Chile applies general search and seizure powers to implement Article 19.2. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.

Party	Legislative and other measures	Assessment
	There is no specific provision for cases where the data sought cannot be determined ("loss of (knowledge of) location situations"). However, Chile specified that its authorities may use the measure only in relation to data that are present on the territory of Chile. In cases when the data are located in a different territory, international cooperation of another State is required.	
Colombia	Colombian regulations do not textually address the problem of locating the system or parts of the system within or outside the jurisdiction for the collection of digital evidence. Nevertheless, Colombia informed that in practice it is done if the data is accessible by the computer expert from a portion of the system that is in Colombian jurisdiction. A written order signed by the prosecutor in charge of the case is required, which must consider the location of the system and the data stored. To be accessed, the data must be accessible by the computer expert from a portion of the system that is in Colombian jurisdiction. If this is the case and the data is accessible, regardless of where it is stored, it is extracted via the portion of the system in national jurisdiction. When this happens, the following procedural rules are observed: i) A written order signed by the Prosecutor is reviewed for legality by a Control Judge within thirty-six (36) hours after forensic activities are completed. ii) The order must specify the necessity, proportionality, and usefulness of the obtained information, including data beyond national jurisdiction, relevant to the specific case. iii) Investigative measures must be conducted to ascertain whether any data falls outside the jurisdiction. To precisely determine whether data may be beyond jurisdiction, investigative actions must be undertaken, including i) Examining the system architecture, ii) Assessing its complexity, location, and critical processes. iii) Identifying stored data. iv) Reviewing technical documentation, active credentials, and associated privileges. Pre-identifying data are potentially relevant as evidence in the case. v) Additionally, the Judicial Police can seek authorization for search extensions via a report to the Attorney General's office, as outlined in Article 209 of the Criminal Procedure Code.	Colombia applies general search and seizure powers to implement Article 19.2. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.

Party	Legislative and other measures	Assessment
	Colombia mentioned that difficulties may arise in this respect when: i) When dealing with a computer incident, the priority is the recovery of the system and not the investigation of what happened, which limits cooperation with the authorities. ii) There is no interest on the part of the administrator in clarifying what happened, so cooperation is abandoned, and the case fails. Considering that Colombia lacks legislation on the matter, it detailed judicial decisions of the Supreme Court of Justice, where these issues have been resolved as follows: When the data is stored outside the national territory but is accessible from a part of the system that is under the custody of the judicial investigation authorities or in any case is accessible by the same entities from the national territory, it is sufficient for the computer experts to indicate in their reports that: i) The activities were initiated based on an order legally issued in Colombian territory. ii) That such activities were carried out within the national territory on a system or portion of a system that by its architecture may have other portions of the system or data outside the territory. iii) That such data or portions of the system are technically accessible from national territory and therefore the data are relevant and insurable from Colombian jurisdiction. Regarding how authorities proceed when the exact location cannot be determined, Colombia mentioned that the main concern is not so much the possibility of precisely identifying the jurisdiction of each part of the system or the concrete storage of the data if it is accessible and preservable from the Colombian jurisdiction through the legal formalities in force. For this case, this interpretation has been made on Article 236 of the Colombian Code of Criminal Procedure, which allows the extraction of data resulting from the transmission of data by the suspect. On the other hand, if the system is not accessible from Colombian jurisdiction as it is located entirely abroad, they indicated that the Supreme Court of Justice has pointed out that judicial cooperation in this matter is necessary to acquire any type of digital evidence. This was done based on the application of the provisions of Articles 484 and 485 of the Colombian Code of Criminal Procedure. Finally, Colombia informed that the lack of compliance with these channels has resulted in the exclusion of material evidence due to illegality in judicial proceedings.	

Party	Legislative and other measures	Assessment
Costa Rica	If during the investigation, or even during the search and seizure of the initial data, it's determined that another piece of hardware (located in Costa Rica) contains important information to the investigation, the judge can extend his warrant to seize and analyse this new data. Then the prosecutor's office and/or Judicial Police will execute the order. In Costa Rica, the "motives to believe" are equated to "sufficient or positive probability", so that when access to information similar to that provided for in Article 19.2 is sought, the Prosecutor must demonstrate in his request to the judge that due to the facts and the evidence available up to that moment, there is sufficient probability that they are in the place where they are indicated, and in turn, the judge in his decision must evaluate and analyse such positive probability, adequately justifying his order. "In its territory" refers to the physical place in which Costa Rica exercises its sovereign powers. In this moment, is required that the system (hardware) that storage the data must be in Costa Rica, or that the provider of the service has an open business office in Costa Rica. There is no specific rule in place for the situations in which is not possible to determine where the data sought are stored ("loss of (knowledge of) location situations").	Costa Rica applies general search and seizure powers to implement Article 19.2. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.
Croatia	Article 257, Paragraph 1 of the Croatian Criminal Procedure Code prescribes that the search and seizure refers to both computer and devices connected with the computer. The search shall be conducted upon court warrant indicating an object of the measure. The extension of the search to that other computer system according to case-law could be conducted either through initial court warrant indicating possibility to extend the search or upon the subsequent court warrant indicating another computer system that should be searched. Grounds to believe should be established either through the location of the connected device, indicated in the reasoning of decision and derived from previously undertaken investigative measures. This mostly depends on factual circumstances of a case. Neither the Code itself, nor the case law, is explicit about whether this provision (Article 257 (1) of the Criminal Procedure Code) applies only to those connected devices which are physically located in the	Croatia applies specific search and seizure powers to implement Article 19.2.

Party	Legislative and other measures	Assessment
	territory of the Republic of Croatia or the search can be extended to the connected devices located in an unknown location/abroad.	
Cyprus	Cyprus can extend searches per Article 19.2 if it procures a further search warrant pursuant to the standard procedures described above. To procure such a further warrant, the authorities must show reasonable suspicion that computer data are stored in another, specified computer system that has not been searched for evidence. Applications for search warrants must include information about the purpose of the search and the items, documents or data sought. Further, they must include specific information about the premises or location for which the search warrant is requested. Therefore, a second search warrant extending a search to a connected computer may be issued if 1) there is information that a crime has been committed and 2) there are reasonable grounds to believe that in a specific premise or area there might be items, data, documents or other evidence linked to the case. If the location of the evidence sought is not known – that is, if there is information that a crime has been committed but no information that a specific premises or location contains evidence relevant to the case – a warrant may not be issued, because it will not be possible to specify in the application for the warrant the location of the items, documents or data or other evidence sought. Cyprus does not assert the right to extend searches outside its territory.	Cyprus applies general and specific search and seizure powers to implement Article 19.2. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.
Czech Republic	The measures concerned include provisions on house search (Provision 83) and search of other premises and places (Provision 83a) both defined in the Criminal Procedure Code (CPC). In case that law enforcement authorities are able to download data from available computer and connected device located in the territory of the Czech Republic, they are competent to act so, unless it is known that those data are located in the territory of foreign State. If data are place in the territory of foreign State, the channel of international judicial cooperation shall be used.	Czech Republic applies general search and seizure powers to implement Article 19.2. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.

Party	Legislative and other measures	Assessment
	Identical procedure applies for extension of searches, as in relation to house search, i.e. Criminal Procedure Code (CPC). Authorisation to obtain access to data available from device in the place of house search is included in the court order authorising the house search. As per the relevant case-law, essential condition for the house search is the reasonable suspicion that in the apartment or other premises used for accommodation or in the premises belonging to it, the item or person important for criminal proceedings is located. The precondition for this is the existence of facts or evidence eligible to convince the objective observer that in the searched premises the respective item or person may be located. The device where the data are stored or from which those are available have to be located in the territory of the Czech Republic and the law enforcement authorities have to be able to download them. If it is known that data are place in the territory of foreign State, the channel of international judicial cooperation should be used. On the other hand, from the reply on typical examples (use cases) it appears that authorities might use the measure also when data are stored on a computer system abroad.	
Denmark	The law assumes that a properly-authorised search includes the content of digital messages that the person concerned has received and that are accessible from the initially-searched computer. A Supreme Court decision has permitted searches when servers with the target data were known to be outside Denmark. If extending a search would require access to new targets, a new court order must be procured. "Grounds to believe" will derive from indicators in the initial search. The approach to situations in which the location of the data is unknown is governed by the Supreme Court decision above. In the verdict, the court noted that the crime was subject to the Danish right of punishment, the case was being investigated by Danish authorities and the search could be conducted without involving any foreign authorities. For these reasons, it was insignificant that the information was physically located on servers outside of Denmark, in this instance in California and Luxembourg. The Supreme Court did not explicitly state that this rule would apply in other similar situations. However, since the physical location of data is often random, the questionnaire response concludes that the location of the data is insignificant if the above-mentioned conditions are met. This conclusion would also be in line with	Denmark applies general search and seizure powers to implement Article 19.2. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.

Party	Legislative and other measures	Assessment
	sections 6 and 9 of the Criminal Code (rules on Danish jurisdiction in criminal cases), pursuant to which it is generally assumed that internet/information crime can be prosecuted in Denmark if it has had an effect in Denmark.	
Dominican Republic	The Dominican Republic indicated that it contains no restrictions in case it has reason to believe that the evidence is in another system connected to or accessible through the system for which the search warrant is initially held. Competent authorities shall act promptly to preserve data contained in an information system or its components, or system traffic data, where they are at risk of loss or modification. Since the legislation does not impose any restrictions in cases where the data are in a connected system or are accessible through the original system, the authorities may carry out searches in adjacent and connected systems. Currently, the criminal procedure code allows officials from the public ministry or the police to conduct searches in places or items when "there are reasonable grounds to believe" that useful evidence for the investigation exists. The legal framework of the Dominican Republic establishes that the concept of "territory" applies in the following situations: i) When the perpetrator or instigator of the offense acts within the national territory. ii) When the perpetrator or instigator of the offense acts from abroad but has effects on Dominican territory. iii) When the origin or effects of the offense are abroad, but means are used in the national territory. iv) When there is complicity from Dominican territory. In cases where the exact location of the data is unknown, a preservation request is made to the service provider, who will indicate the location of the stored data. Finally, it is important to note that there is currently a bill in Congress to amend the Cybercrime Act, which would include remote search powers that could be used in such scenarios.	Dominican Republic applies general search and seizure powers to implement Article 19.2. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.

Party	Legislative and other measures	Assessment
Estonia	There are no limitations in national law to extension of search. It is possible to lawfully access the computer system and extend the search to connected systems. Authorities indicate that provisions on search and examination of an object apply. For the covert access additional court authorisation is required. Legal framework does not define "grounds to believe". It is stated that access needs to be lawful pursuant to the national legislation. Legislation does not require that online search needs to take place in Estonia. Extension of online search in cyberspace is thus not precluded. It is also not required explicitly that the physical location of the data needs to be identified or determined.	Estonia applies general search and seizure powers to implement Article 19.2. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.
Fiji	Fiji reported that legal basis for extension of search is provided in Section 21.3 and 21.4 of the TCA. This provision provides for the following: Where a police officer or other authorized person under this Act is permitted to search or similarly access a specified computer system, program, data, or computer data storage medium, under subsection (1), and has grounds to believe that the data sought is stored in another computer system, and such data is lawfully accessible from or available to the initial system, the police officer or other authorized person may extend the search or similar access to such other system or systems. A warrant of a judge must be issued to authorise this measure. 'Grounds to believe' can only be confirmed after initial searches to verify whether there is a need to extend a search. Lawyers will be guided by technical digital experts. On the question Section 3(2) of the ATT sets out the scope of application of 'in its territory'. It contains a variety of jurisdictional settings, but exclusively found or accessible in Fiji. It was further noted that in cases where it is not possible to determine where the requested data is stored, legal advice is taken, suggesting that a case-by-case approach may be taken. More specifically, if permitted technically by the search warrant, the data may be seized, but if any other technical methods are to be used, then another search warrant must be requested until all technical avenues are exhausted.	Fiji applies specific search and seizure powers to implement Article 19.2.

Party	Legislative and other measures	Assessment
Finland	The CMA contains provisions on searches and covert coercive measures in Chapters 8 and 10. As per these provisions, a search of data contained in a device refers to the search specifically directed towards the data present in a computer, terminal, or other corresponding technical device or information system at the time of the search. It includes other corresponding technical devices or information systems as well. Remote searches can be conducted as a search of data contained in a device when required for the appropriate conduct of a criminal investigation or by the urgency of the matter. The search of data is conducted without using the device present in the premises or the possession of the person who is the subject of the search. In case of an extended search, a new decision needs to be made on searching the data stored in a device. As this decision is typically made by an authorised individual with the power of arrest, and in urgent cases, by a police officer, it has not presented any issues in practice. The request and decision to search data stored in a device usually specify the search target. It is important to note that when searching data from a device, it may be carried out on the data stored in the device at the time of the search. Performing multiple searches of data stored in a device to circumvent the privacy of sensitive communications or the regulations governing interception of telecommunications and monitoring of traffic data is prohibited. The CMA allows for a search of data contained on a device if there are reasonable grounds to believe that the search may lead to the discovery of relevant documents or data. The decision to extend the search to other devices or information systems may result from interviews, material analysis or criminal intelligence operations that provide information about the devices and services used in the offence. The modus operandi of the crime will also influence the scope of the data search. The CMA and the Police Act do not explicitly provide for the territorial competence of the police in cyberspace, but in practice Finland authorities rely on the rules and interpretations of international law. As a rule, police powers only apply in Finland. In practice, this has traditionally meant only servers located in Finland and the data on these servers. Investigations are carried out to locate data, and if the data are likely to be located within the geographical borders of Finland, the police powers apply to the data. In practice, searches for data on a device are sometimes considered on a case-by-case basis, even if the data can be accessed in Finland. No laws have been enacted or instructions or regulations issued on this matter, but the Finnish interpretation is that if the location of the data is unknown and accessible, obtaining the data by national	Finland applies specific search and seizure powers to implement Article 19.2.

Party	Legislative and other measures	Assessment
	coercive measures must be considered on a case-by-case basis. In this case, consent does not need to be obtained, but the search of data contained in a device is carried out as a remote search in accordance with a decision to that effect. The measure may not be carried out if there is a suspicion that the data may be located in a country that may have a negative or aggressive attitude towards the measure. As a general rule, the measure must not infringe the sovereignty of any state.	
France	The CPC provides for the extension of searches into subsequent systems if they are accessible from the initially-searched system. The usual procedures are followed. Two sections of the CPC implement "grounds to believe" as data that are of interest to the investigation and as data (or other items) useful for proving the truth. In principle, according to Article 57-1 of the CPC, systems connected to a searched system may also be searched. It does not appear that investigators have a legal obligation to determine systematically if the data are stored outside the territory. However, if it is known to be outside the territory, French investigators proceed by mutual legal assistance. If investigators know beforehand that data are outside the territory, they may collect it and retain it without accessing it pending the resolution of mutual legal assistance. By contrast, data whose location is unknown may be delivered to whatever screen is being used in the search. The legal focus is not on the location of the server but on the location of the access to the server.	France applies specific search and seizure powers to implement Article 19.2.
Georgia	There is no direct legislative rule that allows extension of searches. However, searches are regularly extended in actual practice, cases that require extension are treated as emergencies and emergency rules are invoked (Art. 112 of the CCP). Rules applicable to general procedural powers described above apply in case of extension of searches. Standards of proof as to the location of data is relevant in respect of initial searches and the same standard applies to the extensions. There is no legislative rule referring to "in its territory" element. According to the judicial practice searches and seizures have been considered to be carried out in Georgia as long as the access to the connected	There is no direct legislative rule that allows extension of searches; however, searches are regularly extended in practice and cases that require extension of searches are treated as emergencies.

Party	Legislative and other measures	Assessment
	computer system was carried out in the territory of Georgia. However, there is no definite clarity on this issue to the date. The legislation nor the judicial practice has addressed this issue of cases when it cannot be determined where the data sought is stored ("loss of (knowledge of) location situations").	
Germany	Section 110 (3) of the Code of Criminal Procedure allows the extension of search to storage media that are physically separate from the original search premises, if they can be accessed from the electronic storage medium if there is otherwise a risk that the data sought will be lost. This includes e-mails stored on the provider's server and it is irrelevant how many intermediate levels there are between the computer in the search object and the spatially separate storage medium. Court order is needed and requires suspicious of an imminent loss of data. In principle, the data must be located on storage media in Germany. But, in cases in which physical storage location cannot be determined, whether the server and thus the data are in Germany or abroad, a storage location in Germany cannot in principle be ruled out in any case. The mere possibility of a location abroad cannot trigger an obligation to provide international assistance. If, however, it is determined that the storage medium in question is located abroad, and transborder search as unilateral direct access to stored data in the country in question is therefore excluded, request for legal assistance must be submitted.	Germany applies specific search and seizure powers to implement Article 19.2.
Ghana	The laws and procedures for search and seizure in general also apply when searches are extended. Section 99(1) of the Electronic Transactions Act allows a law enforcement officer executing a search warrant under that act to make and take away a copy of any program or record held in any computer beyond the initially-searched computer if the officer has reasonable grounds to believe that the program or record is evidence of the commission of another offence. The authorities also pointed out that the officer conducting the search and seizure may also search other computers other than the initially searched computers if the officer has reasonable grounds to believe that the program or record is evidence of the commission of the same offence. This is based on the discretionary principle in the interpretation of statutes which applies in Ghana as a common law country.	Ghana applies a combination of general and specific search and seizure powers to implement Article 19.2.

Party	Legislative and other measures	Assessment
	"Grounds to believe" that data is stored in the territory must be reasonable and substantiated. Normally, the grounds will be established by one or more of the following elements: at the time of the search and seizure, a law enforcement agent has knowledge or reasonably trustworthy information based on which a prudent person would believe that a system has relevant evidence; evidence (including digital evidence) from the investigation indicates a connection between the offence and the second system; technical expertise indicates that evidence may be on the second system; and documentation/records/analysis indicate the same. Ghanian statutes limit Ghana's criminal jurisdiction to its physical territory with certain limited (and common) exceptions (see responses and notes below re extension outside the territory). Applying this framework and determining whether data is within the territory are done by technical analysis, digital forensics, and consultation with experts. Extensive efforts (detailed in the responses) can be made to identify the location of data. When the data cannot be located in Ghana, authorities can proceed pursuant to the Legal Mutual Assistance Act 2010 (Act 807) by seeking the assistance of a Foreign State. However, several of the use cases described in the responses seemed to indicate that searches will be extended outside the physical territory when necessary.	
Greece	Legislative and other measures provide that a search may be extended when the authorities have reasonable grounds to believe that the data sought is stored in another system within the country's territory. The authorities must obtain additional legal authorisation that describes the extension of the search and states its scope and purpose. The legislation ensures that the data is lawfully accessible from the first system. When the search is extended, technical specialists and specialised tools will be available. "Grounds to believe" is typically established by an accumulation of credible evidence. This may include digital evidence, testimony, documents, technical analysis, and information from other investigations. "In its territory" is interpreted to include cloud systems, regardless of where they physically exist, even if outside Greek territory, as long as they are connected to an initially-searched system that is located within the territory of Greece.	Greece applies a combination of general and specific search and seizure powers to implement Article 19.2.

Party	Legislative and other measures	Assessment
	Determined attempts are made to determine the location of data. These efforts may include technical analysis and digital forensics, collaboration with service providers, and international cooperation. The authorities may seek court approval for broader investigative measures. If the location of the data cannot be determined, searches and seizures are authorised and executed as described above.	
Grenada	Grenada has indicated that the current legislation does not provide for this measure. Search warrants to obtain the computer system are specific to a physical place or entity. Additional warrants must be sought when the discovery of additional systems is made while the search or seizure must be specific as outlined in the warrant. The authorities also informed that the element "grounds to believe" is established solely on the merit of the investigating officers' facts in his/her affidavit. The affidavit acts as a preamble for the investigation and may include other sources of information or evidence. The element of "in its territory" applies to the physical location of the system within the jurisdiction of Grenada. Finally, it was reported that if the location cannot be determined after all means of obtaining this information have been used, the process is stopped.	Grenada applies general powers to implement Art. 19.2. Provisions more specific to computer data and systems could permit greater clarity and enhance legal certainty.
Hungary	Two Government Decrees provide for extension of searches to data accessible from an initial system, regardless of the location of the data, as long as security measures need not be circumvented. "If necessary," an order for a new search may be obtained. However, in urgent cases the prosecution service and investigating authority may conduct a search of any evidence that would otherwise be searchable pursuant to an order. These procedures must be justified and the related procedures (creation of a record of the search) are regulated. Reasonable grounds for conducting a search are evaluated based on the facts of individual cases.	Hungary applies specific search and seizure powers to implement Article 19.2.

Party	Legislative and other measures	Assessment
	The Hungarian Criminal Code establishes rules of criminal jurisdiction. When certain crimes are alleged, that jurisdiction may extend to acts committed by non-Hungarian nationals outside of Hungary. Section 9 of the CPC regulates procedures for cases subject to Hungarian criminal jurisdiction. That section allows the authorities to reach systems located anywhere if they are accessible via systems located in Hungary without violating security measures. Thus, searches are permissible (provided they comply with Section 9) when the location of the data is unknown. Evidence gathered in violation of the section is inadmissible at trial.	
Iceland	Authorities refer to previous replies to the questionnaire, it appears that the same conditions apply to extension of a search as apply to search. „In the territory" is not defined by law. The Icelandic legislation does not expressively regulate the jurisdiction to enforce but the general principle of territoriality must be respected. From the use case provided it appears that such measures are applied in practice most commonly probably in relation to data "in the cloud". There are not in place special provisions on the procedure of an extension of a search nor internal rules, but the same conditions apply to an extension of a search as apply to search. The search will have to be within the conditions set out in the court order given for a search. For example, should it become apparent that part of the data was stored somewhere other than directly at the relevant location that a search warrant applies to, an attempt would simply be made to access such data if possible from the relevant computer system, if and to the extent that it seemed consistent with the court ruling. The same principles would apply in relation to establishing grounds to believe as in an initial search and seizure case, i.e. that if there is reason to believe that items, including documents, shall be seized if there is reason to believe that they, or things or information that they contain, are of evidential value in a criminal case, that they have been acquired in a criminal manner or that they may be eligible for confiscation, like stated in Article 68 of the CCP.	Iceland applies general search and seizure powers to implement Article 19.2. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.

Party	Legislative and other measures	Assessment
	How the legal framework applies "in the territory": "Loss of (knowledge of) location situations": The jurisdiction to perform a remote search when it cannot be determined where the data sought is stored is not regulated in the Icelandic legislation. This would be decided on a case-by-case basis. The police would try to establish the location with assistance from international colleagues, and depending on the circumstances request mutual legal assistance and/or the 24/7 network of the Budapest Convention.	
Israel	The Criminal Procedure Ordinance allows computer searches by connecting or communicating with a computer. Thus, the definition of a computer search includes extending the search. Applications for warrants must request authorisation to extend a search. The Ordinance is silent regarding extensions outside the territory of Israel. The legal framework does not explicitly address the "in your territory" or "grounds to believe" elements of Art. 19.2. In practice, the 'grounds to believe' element is fulfilled based on preliminary evidence indicating whether the suspect uses internet services whose servers may or may not be located within Israeli territory. For example, screenshots or other forensic evidence obtained from the victim may show that the suspect communicated with the victim via Instagram or Telegram. When the location of data cannot be determined, a case-by-case approach is taken.	Israel applies specific search and seizure powers to implement Article 19.2.
Italy	The search and seizure activities can be expanded to encompass any IT system that seems to be linked to, and directly accessible from, the primary system. In such instances, according to the jurisprudence of the Supreme Court the two interconnected systems are treated as a single system, following a legal fiction. During a search and seizure activity the judiciary police can formally certify that the system is connected to another one and then proceed with the search. Regarding the phrase "in its territory", Italy does not have any specific legal requirements. In the cases of loss of location situations the judiciary police uses the same approach as if the data was located in the territory of Italy.	Italy applies general search and seizure powers to implement Article 19.2. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.

Party	Legislative and other measures	Assessment
Japan	Articles 99 and 218 of the CPC stipulate that connected media may be seized, subsequent to any data having been copied, if it may be "reasonably supposed" to be used to retain records processed by the initial computer. At earlier stages, searches may be extended by additional warrants. The procedures for extending searches are otherwise the same as for other searches. The "grounds to believe" element of Article 19.2 is determined by the facts of the individual case and the probability that the medium was in fact used to retain the targeted records. Japanese law does not specifically address the issue of "in its territory." Japan's approach is determined on a case-by-case basis. When the location of data is unknown, Japan follows its judicial precedents and Article 32 of the Budapest Convention.	Japan applies a combination of general and specific search and seizure powers to implement Article 19.2.
Kiribati	Section 22 of the Cybercrime Act, subsections 4 and 5, empowers law enforcement authorities executing a search and seizure to extend a search as in Article 19.2 when they have grounds to believe that the computer data sought is stored in another computer system or part of it in the territory and such computer data is lawfully accessible from or available to the initial computer system. The procedure is the same as with searches pursuant to Article 19.1. Law enforcement authorities must issue a written notice to extend such a search. The "grounds to believe" element of Article 19.2 is addressed by section 25 of the Cybercrime Act. Its requirements include that a police officer must be satisfied that specified computer data, including content data and traffic data, is reasonably required for the purpose of a criminal investigation and that there is a risk that such data may be destroyed or rendered inaccessible. The territory in the context of the Cybercrime Act is the jurisdiction of Kiribati, including ships and planes carrying its flag or registered under its law.	Kiribati applies specific search and seizure powers to implement Article 19.2.

Party	Legislative and other measures	Assessment
	Law enforcement in Kiribati tends to stop at the stage when data location cannot be determined. It now has the possibility to reach out to Kiribati's cybersecurity incident response team for its advanced capabilities. This has not been executed to date.	
Latvia	Per Article 219 of the CPC, searches may be extended within the territory of Latvia based on the authorisation by an investigating judge for search of the initial system. A second warrant is not needed and the procedures are as already described. The statute does not define "grounds to believe," but its text tracks the phrasing in Article 19 of the Budapest Convention. The "in its territory" element of Article 19 is included in Article 219 of Latvia's CPC. Part 2.1 of Article 219 of the CPC states that data stored outside of the jurisdiction of any state may be accessed pursuant to the decision of an investigating judge. If its location is determined later in the course of proceedings, Latvia will then communicate with the relevant state.	Latvia applies specific search and seizure powers to implement Article 19.2.
Liechtenstein	Searches and seizures may be extended by procuring a new search or seizure order (for which there are rapid mechanisms). Such a new order is procured in the usual way – that is, on application by a prosecutor and decision by a court. In addition, the National Police may seize objects without a court order when data are at risk of being lost. "Grounds to believe" are normally established by police interviews of suspects or witnesses, IP addresses showing differing location data, workstations that are missing computers, and references in the system to systems that are not present. "In its territory" is understood to mean within Liechtenstein or accessible from a system within Liechtenstein. It appears that its law permits Liechtenstein to search data whose location is unknown if access to the data is possible from Liechtenstein.	Liechtenstein applies a combination of general and specific search and seizure powers to implement Article 19.2.
Lithuania	Searches are extended according to the procedures described above. If a search/seizure has been conducted and accounts and logins are later found during the examination, a separate covert action must be authorised by a court to permit investigators to proceed. "Grounds to believe," "in its territory," and "loss of knowledge of location" are not defined in statute. The usual requirements are followed when the location of the data is not known.	Lithuania applies general search and seizure powers to implement Article 19.2. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.

Party	Legislative and other measures	Assessment
Luxembourg	The procedures utilised to extend a search pursuant to Article 19.2 are the same as those previously described, including the authorisations and investigative techniques applied. The search warrant is issued for a specific natural or legal person, at the address mentioned in the warrant 'or any other place'. This means that the search warrants do not normally need to be extended because they include the words "or any other place." However, if the search needs to be extended to another person, a new warrant is issued. The legal basis for extension of search is Art. 33 concerning the search and seizure in the framework of a flagrant crime, and Art. 65 concerning the search and seizure carried out in the framework of a judicial investigation conducted by the investigating judge. "Grounds to believe" is implemented as follows. Investigating judges and in case of flagrant offences also the public prosecutor, decide which investigative actions are useful for the investigation, subject to the normal bounds of the powers of such judges. Searches must be for the purpose of discovering objects that are necessary or useful to establish the truth or that are liable to confiscation. Searches may be ordered only to corroborate existing evidence or leads relating to a known, specific offence, *not* to search for offences or crimes or evidence thereof. All data stored or accessible in/from the Luxembourgish territory may be accessed and searched (regardless of whether the location of the data is known or unknown).	Luxembourg applies a combination of general and specific search and seizure powers to implement Article 19.2.
Malta	As described above, a warrant from a magistrate is required in order for a search to be extended as in Article 19.2. A warrantless search may be conducted when the grounds listed above are present. "Grounds to believe" is interpreted according to the reasonable suspicion principle. The responses described broad jurisdiction over criminal offences. Investigative power is a distinct issue. In this regard, response 2.3.2 implied that there is no affirmative requirement that a computer system be within Maltese territory.	Malta uses general search and seizure powers to implement Article 19.2. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.

Party	Legislative and other measures	Assessment
	The police make extensive efforts to determine the location of data and to exploit the devices and data that are available. The police will go back to the drawing board to seek any alternative locations that might have been missed and that could help retrieve more data.	
Mauritius	Pursuant to Section 28, applications for searches, and the orders that proceed from such applications, specify the parameters of the intended search. If extension of a search is needed, a second order must be procured. In lieu of "grounds to believe," Section 28 uses "reasonable grounds to believe." According to established case law, reasonableness is evaluated by an objective test that considers all surrounding circumstances. Typically, those circumstances will include witness statements and documentary evidence submitted to a judge via affidavit. The "in its territory" element of Article 19.2 is explicit in Section 28. When the location of data cannot be determined, the Mauritian approach depends on the type of data sought and its possible location. "If it is in some domain, there is a chance of retrieving the data provided it is accessible from Mauritius." Otherwise, the authorities can act only within the limits of their powers under the Act.	Mauritius applies specific search and seizure powers to implement Article 19.2.
Monaco	Monegasque legislation contains provisions allowing a search to be extended to another computer system accessible from the initial system, as part of an authorised search (Art. 255 of the CPC). Extension of a search follows the same law and procedures as described above. The investigative techniques will depend on the type of system and method of access. If the initial search is authorised, it may be extended to another system accessible from the first one. "Grounds to believe" develop from the investigation and the collection of data. Such grounds must derive from sufficient suspicion. The "in its territory" element of Article 19.2 is interpreted as follows: in order to seize computers or data storage media, the hardware must be in the territory. If the hardware is in another (known) country,	Monaco applies a combination of general and specific powers to implement Art. 19.2.

Party	Legislative and other measures	Assessment
	international cooperation would be requested. If data is reachable from Monegasque territory, it is permissible to collect and exploit it, whether its location is in a known foreign country or is unknown.	
Montenegro	Art. 75.2 of the CPC provides that the search and seizure will include computers and similar devices for automatic data processing to which the computer is connected. Obtaining the search warrant from the court is necessary. Furthermore, the request, inter alia, needs to contain the facts indicating the likelihood that reasons for search exist. The authorities have stated that the domestic law does not provide for an affirmative requirement that the connected system must be in the territory of Montenegro and no practical examples are available. It is not clear from the response how the authorities proceed in loss of location situations.	Montenegro applies a combination of general and specific search and seizure powers to implement Article 19.2.
Morocco	At this moment, the extended search of stored computer data is regulated by general rules on search, without discriminating specifically which may correspond to electronic evidence and stored electronic data. Article 101 of the CPC provides that searches may take place wherever items may be found that would be useful in establishing the truth. Extensions of searches are carried out pursuant to the same regulations governing other searches. Some questions did not have a response.	Morocco applies general search and seizure powers to implement Article 19.2. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.
Netherlands	Article 125j of the Criminal Procedure Code contains the power to conduct a network search if, during a search, relevant data appear to be stored elsewhere on a network allowing the person who conducts the search to also search computer networks from computers located at the search premises. The network search may only be conducted to the degree that the network is lawfully accessible to the people who are regularly present on those premises. Article 557 of the Criminal Procedure Code opens the possibility to perform the network search also from another place, such as a police station. The Dutch national framework does not impose an affirmative requirement that the connected and/or root system should be in Dutch territory. Under the current interpretation of international law, the network	Netherlands applies specific search and seizure powers to implement Article 19.2.

Party	Legislative and other measures	Assessment
	search cannot go beyond the Dutch jurisdiction, without a request for mutual legal assistance, provided that the location of the automated work is known. However, if the location is unknown, and cannot be determined with a reasonable effort, the public prosecutor can assume the automated work and/or the data are within Dutch jurisdiction.	
Nigeria	Section 45 of the Cybercrimes Act (see particularly 45 (2) (e)) authorises the extension of searches under warrants pursuant to that Act. Procedures under that section are described above. When systems are seized and investigation links evidence to another relevant system, the warrant can be extended by amendment of the initial court order or by seeking a second order. Whether a second court order is needed will depend on the manner in which the initial order was made. If the initial order covered only a particular computer device or system, a second court order extending to the new device or system would be required. However, where the initial order is in the nature of an omnibus one, it may not be necessary to obtain a second court order. For example, the court may make an omnibus order as follows: "an order ... permitting officers of the ICPC to enter, search and seize the laptop marked HP-24J-C234 in the office of the Accountant-General and any other computer or electronic device or system connected thereto and used in the operations of the GIFMIS platform." Here, without the bolded phrase, the officers would be limited to the search and seizure of the laptop marked "HP-24J-C234." "Grounds to believe" is decided by the court as a matter of objective evaluation of the facts presented to it. "In its territory" is a question of jurisdiction, also evaluated by the court. If the location of data cannot be determined, an officer may request that the court make an omnibus order. Using the example above, the omnibus order could be as follows: "an order ... permitting officers of the ICPC to retrieve ... (mention/describe nature of the data) wherever it is located or may be found."	Nigeria applies a combination of general and specific search and seizure powers to implement Article 19.2.
North Macedonia	The measures and procedures for extending a search are the same as described above. "Grounds to believe" is implemented by evaluating previously obtained evidence to ensure that a search will lead to the necessary evidence, taking into account the right to privacy.	North Macedonia applies a combination of general and specific search and seizure powers to implement Article 19.2.

Party	Legislative and other measures	Assessment
	The legal framework recognises the Budapest Convention directly and thus incorporates the "in its territory" element. There was no direct response to question 2.2.5 about procedures when the location of data is unknown. However, the response to question 2.3.2 indicated that the same procedures (and the same CPC articles) apply when searches are extended *and* when the location of data cannot be determined.	
Norway	The CPC allows searches and seizures without a court order, but on the order of a prosecutor or a police officer on the scene, in urgent cases. Such decisions must be documents and may require ratification by the court. Such warrantless extensions may involve searches in computer systems, data and storage media. Depending on the case, investigators may instead seek a subsequent court order covering the extension. "Grounds to believe" is understood in Norwegian law generally as meaning "more likely than not" that the accused has committed the relevant criminal offence. "In its territory" may be understood as applied in the Tidal case, which Norway has supplied. In that case, the relevant data was accessed via a coercive measure commenced on Norwegian soil against a Norwegian company with offices in Norway. The decision was made by Norwegian courts maintaining rule of law guarantees. The search gave access only to data that the company itself had stored and could freely retrieve from storage abroad. The data remained unaltered on the foreign server. When the location of the data is unknown, officials decide on a case-by-case basis about how to proceed.	Norway applies general search and seizure powers to implement Article 19.2. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.
Panama	Currently, there is a draft law pending discussion in the National Assembly of Deputies, which provides for data search measures, regardless of its location (within or outside the territory) as long as the required data are publicly available in Panama and the person authorised to disclose it in the foreign country gives his legal and voluntary consent to disclose it (art 338-C of draft Law 632). This bill is currently in the Committee on Government, Justice, and Constitutional Affairs and has not progressed to other stages.	Panama applies a combination of general and specific search and seizure powers to implement Article 19.2. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.

Party	Legislative and other measures	Assessment
	The Panamanian authorities informed that the legal basis for the extension of the search would be the previously mentioned articles: Article 310 and Article 314 of the Criminal Procedure Code. If it concerns a data seizure conducted after a search has been conducted with the presence of the defense, the expansion of the search will be subject to subsequent oversight. In the case of private documents or correspondence, it could be argued that there is a risk of evidence loss, and the procedure would also be carried out with subsequent oversight by the Judge of Guarantees. Panama legal framework applies the "grounds to believe" considering that the procedural law imposes on the prosecutor the duty to carry out an objective investigation, i.e. that which is favourable and unfavourable to the accused or to those interested in the outcome of the investigation (art. 24 of the Procedural Code). Panama legal framework applies the "in its territory" in accordance with Articles 310, 314 and 317 of the Code of Criminal Procedure of the Republic of Panama, for the inspection of data in a computer system, as a requirement imposed by Panama legislation, is the authorisation by a Judge of Guarantees and the due notification of all the parties involved to safeguard constitutional rights and guarantees. The Panama procedure in cases when it cannot be determined where the data sought is stored ("loss of (knowledge of) location situations") is with searches that are performed by key words or phrases contained in the documents or database (from page 62 of the Guide to Expert Services).	
Paraguay	As a result of best practices, technical operations and expertise are conducted, and when there is a possibility to expand searches, extensions of the technical operations are carried out. Similarly, expert points that need to be addressed are expanded, which is determined by the Criminal Court involved in the process and executed by the experts, in accordance with the investigative guidelines provided by the Public Ministry. The procedure for extending a search or similar accessing to another system in practice is outlined as follows: Obtain a search warrant and seize electronic and ICT-related devices; Conduct an analysis of the types of devices seized and perform a superficial analysis of the potential data stored on the devices and the computer systems and data processing capabilities they possess. Based on this analysis, make a request	It appears that authorities rely solely on practice to implement Article 19.2. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.

Party	Legislative and other measures	Assessment
	to the relevant Criminal Judge specifying the believed stored information, such as the type of data, document files, audio and/or video files, or other types of files like executables, etc. The expression "Grounds to believe" is referred to the complaints, the analysis of the events that occurred, according to the possibilities of action provided by the seized object, such as the possibility of data storage and the communication capacity through the device, whether by telephone network or internet etc. The expression "in its territory" refers to the procedural legislation of all matters traditionally requires the implication of the element of territorial jurisdiction in the process. The legislation does not mention that it must be connected in the territory, but by procedural laws, the place of the event must be consigned. In relation to the extent of the search, it is a matter of discretion of the Investigating Prosecutor, but this situation is based on the framework of the application of the Objectivity Criterion that is regulated in "Article 54.	
Peru	Title X of the Criminal Procedure Code establishes the circumstances for extending a search, and Article 19.2 validates such expansions. The Prosecutor must subsequently request authorisation from a Judge, providing necessary premises, to authorise the measure restricting rights through a reasoned judicial resolution confirming the seizure of assets. This provision for the extension of physical space searches is used by analogy for data search. It's important to note that when conducting rights-limiting measures such as "inspection" and "seizure" on properties containing stored computer data and data storage media within the national territory, there is the provision to extend the search or investigation, including the seizure of the objects under investigation for validation. This extension is carried out in accordance with the provisions of the Criminal Procedure Code. Additionally, it is permissible to request judicial validation in cases where the initial judicial authorisation for "inspection" and "seizure" does not specify a particular location for the measure's execution. In practical terms, this means that the Prosecutor, acting under a judicial resolution, can prolong the rights-limiting measure during its execution to broaden the scope of the investigation. For example, if a search warrant is issued for a specific residence but evidence suggests a connection to neighbouring residences not covered	Peru applies general search and seizure powers to implement Article 19.2. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.

Party	Legislative and other measures	Assessment
	in the initial authorisation, the search of these neighbouring properties can be continued. For further clarification on this matter, reference can be made to Articles 214°, 217°, 316°, and 318° of the Criminal Procedure Code, which pertain to inspection, search, and seizure. The validation of the requirement on the confirmation of seizure of property has a procedure provided for in Title X of the Criminal Procedure Code. The measures restricting rights are applied to computer data stored and data storage media in the territory, these restrictive measures of law such as search and seizure are developed in a specific space as prescribed in the Criminal Procedure Code, however, according to article 316 of the Criminal Procedure Code, the seizure may also be applicable as a measure of coercion (establishing a precautionary function) on the property during the preparatory investigation stage that has not been previously required by the Prosecutor. The element "reason to believe" is related to the varying degrees of suspicion addressed in the national legal system. In this sense, the initial suspicion required by the Prosecutor to initiate preliminary proceedings in response to criminal information is a crucial factor in the search for data. The guides for collecting digital evidence also serve these purposes during the investigation. The element "in its territory" is limited to the provisions stated in the cited article of the Constitution; In this context, no requirements are imposed that affirm the connection of the systems in the national territory. However, when servers are located outside the national territory, other mechanisms of international law are applied for information requests. Although it is not expressly provided for in the Law, the Peruvian authorities have interpreted that In cases where the location of stored data cannot be determined, the Criminal Procedure Code allows for the continued collection of information, even if the data's location is unknown at the time of requesting authorisation for the restrictive measure from the judge. In this regard, Peruvian procedural rules expand the scope for obtaining data.	
Philippines	Searches may be extended using the same processes and with the same requirements described above. A new warrant is not required in order for law enforcement to conduct an extended search.	The Philippines applies specific search and seizure powers to implement Article 19.2.

Party	Legislative and other measures	Assessment
	Law enforcement in the Philippines must not only have "grounds to believe" but must be certain that the data sought to be searched is lawfully accessible from or available to the initial system that is subject of the warrant. "In its territory" is interpreted to mean that a part of the targeted computer system must be within Philippine jurisdiction. Searches may be conducted (within the usual strictures) as long as a targeted system is connected to the initially searched system, regardless of the physical location of the second system.	
Poland	As described more fully above, a search may be extended in urgent cases, subject to later ratification. See Article 220.3 of the CPC. It appears that searches may be extended *only* in urgent cases, but "urgent cases" seem to be defined very broadly. "Grounds to believe" is understood as verifiable information – information from sources that could constitute sources of evidence in criminal proceedings – that has been obtained in the course of an investigation and documented appropriately. Such information should indicate that suspects or items that may constitute evidence are present where expected. The legal framework does not impose an affirmative requirement that the connected system be within Polish territory. The usual procedure for extending a search is used when the location of the data is unknown.	Poland applies a combination of general and specific search and seizure powers to implement Article 19.2.
Portugal	According to Article 15 of the Cybercrime Law, an initial search may be extended to another system, or a different part of the initial system, if the data are legally accessible from the initial system. Such extension requires the authorisation of the competent authority. In planning for a search and issuing an authorising order, it is good practice prospectively to include permission for extension of the search. Searches may also be extended by the police in urgent cases within the restrictions described above.	Portugal applies specific search and seizure powers to implement Article 19.2.

Party	Legislative and other measures	Assessment
	"Grounds to believe" is not defined in statute. In each case, prosecutors must determine whether the facts meet the standard in the Cybercrime Law: whether it is necessary to gather evidence to ascertain the truth. Searches may be extended regardless of the location of the remote system or if the location of the data is unknown. The legal framework does not apply "in its territory" to such extensions.	
Republic of Moldova	There are no specific legislative measures regarding extensions of search. However, Moldova uses Article 125/4 of the CPC when searches need to be extended. As noted above, that provision allows searches based on a reasoned order of a public prosecutor, subject to the investigating judge's ratification of the action, in cases not subject to postponement or in cases of flagrante delicto. Under Article 125 of the CPC, a warrant to access data may issue if there are reasonable grounds to suspect that the data will constitute evidence. The "grounds to believe" that data may be stored in another system in the territory may be provided by forensic experts who assist in the search and seizure. Searches are restricted to the territory of Moldova. Certain CPC articles relating to international assistance may be relevant. However, Moldova's responses also indicate that it has the power to search when the location of the data is unknown (a second warrant may be sought).	Moldova applies general search and seizure powers to implement Article 19.2. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.
Romania	Under Article 168 of the CPC, if it is determined during a search that the target data are in a system or storage medium accessible from the initial searched item, the target data are copied and preserved, and application is made to extend the warrant. Art.168 does not refer to the location of the other computer system or device, the only condition is that the data in another system or device must be available from the initial searched system. An unknown location is irrelevant since the text assumes that the data are accessible from the initial location disregarding the targeted data location. Computer searches are not performed live but under lab conditions with no Internet connection. Because the computer search is performed under lab conditions with no Internet access, extension of the search is unlikely.	Romania applies specific search and seizure powers to implement Article 19.2.

Party	Legislative and other measures	Assessment
	"Grounds to believe" is not used in the implementing statute. Instead of "grounds to believe," the statute uses "it is found that the data sought is on another…" Prosecutors must demonstrate that the target data were found in another computer system accessible from the initial system.	
San Marino	San Marino informed that there is no specific legislation or case law for the search and seizure of stored computer data in San Marino. Consequently, these matters are not explicitly regulated, and they are addressed through the application of analogous legal principles. In accordance with Article 68 of the Code of Criminal Procedure, if the nature of the crime is such that it is plausible to obtain evidence by means of documents or objects held by the suspected person, by other persons or in places where they are presumed to be concealed, a search may be conducted to find them. If a delegated search identifies data in a location other than the one specified in the judicial decree, but the decree states that "the data shall be searched wherever they are located," the relevant authorities can extend the search to other reasonable locations. If the decree in question specifies a particular location, such as a house or server, the police are unable to conduct a search in any other location without the issuance of a new decree. In such instances, the information is promptly conveyed to the presiding judge, who may then authorize additional searches. However, when it comes to interpretation of the term "in its territory", the authorities pointed out that taking into consideration the absence of a specific regulation and a consolidated number of case law precedents, it must be assumed that the computer system subject to the measure must be physically located within the territory of the Republic of San Marino. If it is necessary to search a computer system that is connected to the system present in San Marino, but located outside its territory, a formal request to the foreign State concerned shall be followed.	San Marino applies general search and seizure powers to implement Article 19.2. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.
Senegal	Pursuant to the 2016 amendments, CPC Articles 90-2 and 90-3 provide for the extension of searches to a system other than the initially-searched system (as specified in Article 19 of Budapest). Subject to applicable international arrangements, a judge may collect stored data in a system other than the initial system located in another place on or outside Senegalese territory, assuming that the subsequent	Senegal applies specific search and seizure powers to implement Article 19.2.

Party	Legislative and other measures	Assessment
	system is accessible from the initial system. Such extension must be necessary to determining the truth or there must be risks of loss of evidence without the extension. The extension must reach only those systems to which persons authorised to use the initial system have access. The judge must inform the person in charge of the system unless their identity or address cannot be found. The law does not include a definition of "in its territory" or "grounds to believe." Judges must define and apply these concepts. Nevertheless, it appears that the concept of "national territory" can be derived from its constitutional meaning: a limited space in which a State exercises its sovereignty. "Grounds to believe" in the Article 19 sense could include a totality of elements or facts indicating that it is likely that stored data in a system beyond the initial system could contribute to determining the truth.	
Serbia	There is no specific statute regarding extensions of searches. However, when it becomes apparent during a search that an extension is advisable, an urgent request for extension will be made to the on-call duty pre-trial judge. "Grounds to believe" that data is stored in a connected system are established by electronic evidence and electronic evidentiary leads during the initial search/seizure. The CPC restricts the reach of the Criminal Code to the territory of Serbia with a few limited exceptions based on treaties and under strict conditions. In most cases in which the location of data cannot be determined, law enforcement will extend the search/seizure to that data, provided that there was an order for the initial search/seizure and that the targeted data is reachable by legal means.	Serbia applies a combination of general and specific search and seizure powers to implement Article 19.2.
Sierra Leone	Sierra Leone authorities reported that section 10 (5) of the Cybersecurity and Crime Act 2021 makes provision for extended search. Where an enforcement officer or authorized person authorized to search or access a specific computer system or part of it has a reasonable ground to believe that the data sought is stored in another cloud computer system and there is reasonable ground to believe that such data is accessible from or available to the initial system, the enforcement officer may extend search or access to such other system.	Sierra Leone applies specific search and seizure powers to implement Article 19.2.

Party	Legislative and other measures	Assessment
	The authorities reported that they use the same warrant for search and seizure and that their procedures apply under Section 10 of the Act. Sierra Leone's legal framework applies 'grounds to believe' in the following manner: In an application for a warrant to access specified data stored in another computer system or part of it, the executing officer must state the grounds to believe for the application. The officer the reasons why it is believed that an investigative search may be frustrated or prejudiced unless an investigation officer has access to them. The authorities reported that the warrant sought in Section 10 applies only to the territory of Sierra Leone, although there is no affirmative requirement that the connected system be located in Sierra Leone. There are no cases available when it cannot be determined where the data sought is stored ("loss of (knowledge of) location situations").	
Slovak Republic	The Slovak Republic cites Sections 91 and 116 of the CPC as the basis for extension of searches. It does not appear to address this issue, but the responses also indicate that extension of searches can be authorised by procuring an order to search a subsequent system. Implementation of extension of searches through the quoted provisions requires more clarification. "Grounds to believe" are established by evidence other than the target evidence, per the CPC, or from information obtained from other investigation. The term is not defined in statute. The CPC does not explicitly provide that a connected computer system be located within the Slovak Republic. "In its territory" is defined in the Criminal Code. The Slovak Republic will not carry out search and seizure on data that is not located on its territory. In such cases, it acts either based on treaties or without a treaty basis pursuant to Chapter Five, Part Five, of the CPC (not provided). The responses did not address cases in which the location of the data cannot be determined.	Slovak Republic applies specific search and seizure powers to implement Article 19.2. However, more clarification on the applicable legal basis would be desirable.
Slovenia	Article 219a of the CPC authorises the search of electronic devices accessible from an initial searched item, assuming that the initial search complies with the legal requirements. If the initial warrant explicitly	Slovenia applies specific search and seizure powers to implement Article 19.2.

Party	Legislative and other measures	Assessment
	mentions the possibility of extending the search, that warrant will suffice to authorise the extension. Otherwise, a subsequent warrant must be obtained under the same rules as applicable to the first warrant. "Grounds to believe" is implemented as a probability that a criminal offence has been committed. There must also be probability that the targeted electronic device contains electronic data based on which a target can be identified, etc., or that evidence of a criminal act will be discovered that is relevant to or usable in the criminal proceedings. Probability is judged on the totality of the facts, including that devices or systems are connected. The legal framework does not explicitly impose an affirmative requirement that a connected electronic system be in Slovenian territory, nor does it address the issue of undermined location of data. Article 219a of the CPC was recently updated to allow for the extension of searches into connected devices and systems.	
Spain	Article 588 sexies c 3 of Criminal Procedure Code allows access to a second computer system with judicial authorisation only, when the information sought is hosted on that system and can be lawfully obtained from the initial device under investigation. Article 588e(c) requires a new judicial decision for the extension of a search, which must be justified in the same way as the initial authorisation. In urgent situations, officers can act without prior judicial authorisation but must inform the court within 24 hours and justify the urgency. The judge must validate or revoke the measure within 72 hours. If the evidence is stored in the cloud and the type of file is known, officers can act from the computer where the intervention begins. A simple search can be done by viewing and downloading the evidence, while a complex search may require specialized forensic software. If the data of interest are hosted on a platform managed by a service provider, officers can request preservation while waiting for judicial authorisation. The content of an email account can be accessed regardless of where the email manager's servers are located if it can be accessed from a system with judicial authorisation. In some investigations, physical access to a server may be necessary, requiring international police and judicial collaboration. The term "grounds to believe" is defined in Article 588 sexies c.3º Criminal Procedure Code (LECrim). as "founded reasons to consider," which is used when there are indications that the investigator is using a second system containing relevant investigation data. Law enforcement must inform the judicial authority	Spain applies specific search and seizure powers to implement Article 19.2.

Party	Legislative and other measures	Assessment
	and request permission to search the second system if it has not already been granted for the first order. If there is a suspicion that a second system may contain relevant data and is interconnected with the first, judicial authorisation is likely to have been requested at the beginning of the investigation to access both systems. This scenario does not limit the exercise of extended registration, and according to Spanish legislation, does not require knowledge of the location of the targeted system is not a prerequisite if there exist rational indications that pertinent data are stored within.	
Sri Lanka	Extensions of searches are governed by Part II of the CCA – that is, the same procedures utilised for searches under Article 19.1. Authorisations and investigative techniques are the same. "Grounds to believe" that targeted data is stored in a connected system in the territory are also governed by Part II, but the specific section is unclear. The "in its territory" element is implemented by the procedure in the Judicature Act no 2 of 1978. In cases where the location of data cannot be determined, the relevant investigating authority will have discretion to decide how to proceed.	Sri Lanka applies a combination of general and specific search and seizure powers to implement Article 19.2.
Sweden	Sections of the CPC provide that searches may be extended. There are two bases for extending a search: a) in a readable information system that the person reasonably suspected of the offence is likely to have used, the authorities may search for information of potential importance to the investigation; or b) the authorities may conduct a search if there is extraordinary reason to assume that information of potential importance can be found. An order authorising such searches may be issued by the leader of the investigation, a prosecutor, or a court. If the search will be extensive or cause extraordinary inconvenience, the search should be conducted only pursuant to an order issued *by a court* unless the delay would entail risk. In that case, the police may proceed without an order. The execution of searches is conducted by the investigating authority, ideally in cooperation with experts in digital forensics or other specialised personnel. Especially complex cases are handled by experts at the National Forensic Centre of the Police Authority.	Sweden applies a combination of general and specific search and seizure powers to implement Article 19.2.

Party	Legislative and other measures	Assessment
	The general principle of territoriality must be respected. The legislation on coercive measures does not expressly regulate the "in its territory" element. This element has not been regulated regarding remote search either. The law concerning obtaining electronic data physically stored outside Sweden is developing. Legislation has been proposed to address this issue in certain cases. Further, the Supreme Court decided in March 2023 that remote searches extending into foreign states were permissible under certain conditions (see case report supplied by Sweden). These conditions include that the search be conducted using equipment located in Sweden and that the data not be deleted or its content affected. Such searches may be conducted both when the location of the data is unknown and when the authorities know the country in which the data is stored.	
Switzerland	It is permissible to extend a search from a lawfully-searched initial computer to accessible data in a subsequent connected system or storage. This extended search must be authorised by the initial warrant or a new one. Cloud data reachable from the initially-searched node are considered to be covered by the first warrant. "Grounds to believe" is implemented based on concrete evidence suggesting the existence of necessary and relevant data as well as the usual prerequisites of sufficient suspicion, proportionality, and reasonableness of the respective measure. According to the jurisprudence of the Supreme Court, an account and data may be searched if accessible from Switzerland even if they are located outside its territory (always assuming that the prerequisites have been met). This ruling also governs the cases in which the location of the data is not known.	Switzerland applies a combination of general and specific search and seizure powers to implement Article 19.2.
Tonga	No legislation specifically addresses the extension of searches, but the search and seizure provision of the Computer Crimes Act, via its definition of computer system, allows extension of the search per Article 19.2. The usual procedures for searches under Article 19.1 are also applicable for searches under Article 19.2.	Tonga applies a combination of general and specific search and seizure powers to implement Article 19.2.

Party	Legislative and other measures	Assessment
	"Grounds to believe" is expressed as "reasonable grounds to suspect" in Section 9 of the Computer Crimes Act. Magistrates decide whether the evidence adduced in a police application and supporting affidavit meets the standard. At present, the "in its territory" element is interpreted to mean that only data or systems physically within Tonga may be searched. Connected systems, data, etc, outside of Tonga may not be searched even if accessible from Tonga. Tonga hopes to enact a new Computer Crimes bill that would allow extension of searches beyond its physical territory. Tonga makes extensive efforts to locate data. It did not respond regarding its approach when the location of data cannot be determined. (see question below).	
Tunisia		
Türkiye	Data that are stored in a system accessible from an initially-searched system may also be searched. The additional system must be considered to be used by the suspect. The usual procedures are employed, and the usual justice officials are involved. Under Article 134 of the CPC, the basis for a warrant must be strong suspicion based on concrete evidence, with no other way to obtain the evidence. If a system "used by the suspect" is in another country but accessible from a computer "used by the suspect" at the initial search site within Türkiye, the extended search is considered to take place within Türkiye (assuming that the usual procedural requirements have been met). It appears that this is the approach when the location of the data is unknown. Searches extending into another country from other sites – for example, a police lab – are considered unauthorised access.	Türkiye applies specific search and seizure powers to implement Article 19.2.
Ukraine	There is no specific rule to comply with art. 19.2. The possibility appears to arise from an application of the general rules.	It appears that Ukraine applies general search and seizure powers to implement Article 19.2. Provisions specific to computer data and systems

Party	Legislative and other measures	Assessment
	Ukraine interprets that the element of Article 19.2 "on its territory", which includes that the connected system be on the territory of Ukraine, not impose an affirmative requirement in the legislation of Ukraine.	could permit greater clarity and enhance legal certainty.
United Kingdom	The UK authorities informed that PACE does not permit the automatic extension of a search to different premises and in some cases a new search warrant will be required. In some cases, a search warrant can be issued for all premises controlled by a person specified in the application for a search warrant, in which case a search can be extended to another computer system located in those premises. Where electronic information is accessible from premises, a constable can require production of this material "in a form in which it can be taken away and in which it is visible and legible or from which it can readily be produced in a visible and legible form." The same approach appears to be used under the Police and Criminal Evidence Order (applicable to Northern Ireland) of 1989 that relies on general powers. In Scotland, no specific power to extend searches exists. The procedure would be the same as for the initial instruction to examine the first device. For access to a remote system where, for example the device has been removed from the premises, then a TEI under the IPA 2016 may be required. To the "grounds to believe" element of Article 19.2, the UK authorities informed that PACE in general applies in England and Wales and searches under PACE are authorised for premises located in this jurisdiction. IPA warrants have extraterritorial effect, for TEI this is covered in sections 126 and 127 of the IPA. For Scotland, to the extent that this is relevant, the powers of Sheriffs or a Justice of the Peace to grant warrants is limited by matters of jurisdiction. The way in which UK authorities proceed when it is not possible to determine where the data source is located is an operational decision for law enforcement agencies, depending on the circumstances of the investigation.	United Kingdom applies a combination of general and specific search and seizure powers to implement Article 19.2. Provisions specific to computer data and systems establishing a legal framework for the search and seizure of computer data and systems applicable in England, Scotland, Wales and Northern Ireland could permit greater clarity and enhance legal certainty.

Party	Legislative and other measures	Assessment
United States	Warrants are issued to search items located in the judicial district where the issuing judge sits. To search data located in a different judicial district but accessible from the initially-searched device, the authorities must obtain another warrant in the second district. Alternatively, if the data are held by a service provider, it may be obtained with a warrant under a certain statute. There are no special procedures or legal bases for extending a search; the usual warrant procedures are used. "Grounds to believe" is implemented via establishing probable cause that the targeted item will be found in the place to be searched and specifically describing that place and what should be seized. US jurisprudence regarding jurisdiction requires that a service provider have minimum contacts with the US before law enforcement may enforce a requirement to disclose data (pursuant to the appropriate warrant). A federal judge may issue a warrant to access electronic storage remotely and to seize its data, regardless of whether the storage or data is in the judge's district, when the location of the data has been concealed through technological means.	The United States applies a combination of general and specific search and seizure powers to implement Article 19.2.

6 SEIZURE OR SIMILARLY SECURING COMPUTER DATA ACCESSED (ASSESSMENT OF ARTICLE 19.3)

This section assesses implementation of Article 19.3:

> Article 19 – Search and seizure of stored computer data
>
> 3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:
>
> a seize or similarly secure a computer system or part of it or a computer-data storage medium;
> b make and retain a copy of those computer data;
> c maintain the integrity of the relevant stored computer data;
> d render inaccessible or remove those computer data in the accessed computer system.

6.1 Implementation of Article 19.3: overview

6.1.1 Legislative and other measures, procedure for seizure – summary

Many Parties had some difficulty in describing their capacity to fulfil the requirements of Article 19.3 and were requested to provide further information to clarify how Article 19.3 was implemented. It was assumed that Parties in fact had the necessary powers and merely needed to explain the basis for the powers.

There are four elements in Article 19.3:

- seizing and securing a computer system or part of it or a computer-data storage medium,
- copying and retaining computer data,
- maintaining its integrity, and
- removing it or rendering it inaccessible.

6.1.1.1 Seizing or similarly securing a computer system or part of it or a computer-data storage medium

Almost all Parties can seize computer hardware and computer data storage media and no significant issues were encountered in the assessment as regards this element. Since computer hardware and storage media in most jurisdictions are considered tangible objects, Parties may use their traditional search powers to seize them.

Examples of practices include:

- Georgia: Grounds for seizure

  An item, document, substance or any other object containing information essential to the case, may be seized if there is probable cause that it is kept in a certain place, with a certain person and if there is no need to search for it.

- Japan: relevant case-law

The Supreme Court held that where it is probable that information related to the alleged facts of the crime is recorded in a recording medium, and where there is a risk of damaging the recorded information if the law enforcement authority inspects at the scene whether such information is actually recorded, it is permissible for the law enforcement authority to seize the said recording medium without inspecting the contents of the medium at the scene.

- Lithuania:

  If it is necessary to seize objects or documents relevant to the investigation of a criminal offence and it is known exactly where they are or who has them, the pre-trial investigation officer or prosecutor may carry out a seizure. If the objects or documents are to be seized, the public prosecutor shall submit a reasoned application for seizure, on the basis of which the court shall authorise or refuse the seizure.

6.1.1.2 Making and retaining a copy of computer data

In the course of answering about making and retaining a copy of the computer data, most Parties[55] noted that they had such power. Most often, Parties stated that this power derived from general procedural powers, from a statute specific to electronic data, or from practice, including written guidelines[56].

Examples of practices on making copies of computer data instead of seizure:

- France: on the spot copying

  Computer data may be seized either by placing the computer system or computer-data storage medium on which the data are stored (e.g. computer, tablet, telephone, hard drive, USB stick, etc.) under court supervision, or by making a copy in the presence of the people who are required to be present during the search. In the latter case, the public prosecutor (or investigating judge) may subsequently order the permanent deletion of the data on the computer system or data-storage medium that has not been placed under judicial supervision.

- Norway: on the spot copying

  The storage medium or a device containing storage media may be seized, or the information from a storage medium may be seized by copying it on the spot. Copying can be done by mirroring or file copying and a back-up must be made and retained for the same length of time as the mirror/file copy.

- Spain: copying to minimise harm

[55] Albania, Australia, Austria, Belgium Bosnia and Herzegovina, Brazil, Bulgaria, Cabo Verde, Canada, Cyprus, Czech Republic, Dominican Republic, Estonia, Fiji, Finland, France, Georgia, Germany, Ghana, Greece, Hungary, Iceland, Israel, Japan, Latvia, Liechtenstein, Lithuania, Mauritius, Netherlands, Norway, Panama, Paraguay, The Philippines, Portugal, Republic of Moldova, Senegal, Sierra Leone, Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Tonga, Türkiye, United Kingdom, USA.

[56] For example, Israel indicated that specific procedures for search and seizure are further elaborated in State's Attorney Guideline no. 7.14 on the Principles of Action Concerning the Seizure, Search, Copy and Examination of Computers and Computer Data. Norway pointed out that the Police Directorate instructions in Circular 2010-7 entitled "Processing of seizures in criminal proceedings" further describe the process of seizing objects containing data.

Seizure of the physical media may in some cases cause harm to the owner of the data. In such cases, copying of the data may be advisable, ensuring appropriate conditions of authenticity and integrity. The judicial body decides whether to seize the device or make a copy of the content, this usually depends on the circumstances of the ongoing investigation. If the device is for the sole use of the respondent and if the illegal content is voluminous (as in cases of child sexual abuse material), the device is usually physically seized for a full examination of the device. However, if it is, for example, a criminal activity carried out from the computer system of a company that is not in fact involved in the unlawful action, the copying system is usually used.

Examples of practices on making copies of computer data after the seizure – making and retaining a copy to preserve integrity of the data:

- Paraguay: If the seized digital is at risk of being altered or disappearing, or if it is difficult to keep or perishable, reproductions, copies or certifications of their existence will be made and maintaining their condition will be ordered.

- Slovenia: After an electronic device is seized, the data are secured in electronic form by storing it on another suitable data carrier in such a way as to preserve the identity and integrity of the data and the possibility of its use in the further process, or an identical copy of the entire data carrier is made.

- Romania: In order to ensure integrity of the computer data stored on the seized objects, the prosecutor orders the making of copies of them.

6.1.1.3 Maintaining the integrity of the relevant stored computer data

Maintaining the integrity of evidence is a routine part of criminal procedure. Perhaps because it is taken for granted, Parties often had difficulty explaining the source of their power to maintain the integrity of seized data. Eventually, most Parties indicated that this power derived from general procedural powers, from a statute specific to electronic data, or from practice and/or guidelines. Several Parties pointed out that their competent authorities have adopted policies or procedures regarding the "chain of custody" of evidence (including electronic) in criminal investigations and proceedings.

Some Parties also mentioned various periods during which the data should be stored. For example, in Montenegro, the data (considered as objects) may be detained at the longest for 2 months. In the Philippines, by contrast, the law enforcement authorities may request an extension of time to complete the examination of the computer data storage medium and to make a return thereon but in no case for a period longer than thirty (30) days from date of approval of the measure by the court. In Canada, the data may be stored for three months, unless an extension is granted by a justice to store the data up to one year.

Examples of practices include:

- Austria:[57] The seized data carrier has to be forensically backed up depending on the type and scope of the data. This backup always has to take the form of an image backup. A partial backup can also be carried out in individual cases. An image backup will serve as the basis for creating a working copy, which will be subject to investigations/searches. Such an image is created using appropriate forensic security

[57] "Guideline for the handling of seized objects" adopted in Austria sets out more general and legal aspects of (among others) seizure of devices for storage of electronic data (see Appendix; available in German language and not publicly available).

mechanisms (read-only, write blocker). The hash value ensures data integrity: It refers to the data content of the backed-up medium at the time of the backup and the data content of the created image, and serves to prove the immutability of the image.

- Czech Republic: Securing is always carried out in a way that makes it demonstrable that the data have not been interfered with (detailed protocol of action, sealing, presence of a third uninvolved person, etc.). The seized media devices are sealed (placed in a designated container, described, photographed, etc. – recorded). Seizure of data can also take place in a non-physical form, in which case a so-called "hash" is usually used, a checksum which uniquely identifies the seized part of the data and is practically analogous to sealing. The hash is included in the record as an unmistakable identification of the item seized. Files, folders, hard drives and more can be cloned. In practice, if possible, the original disk should be kept in a safe place and only taken out for cloning where necessary.

- Senegal: Independent of the duty imposed on the authorities to maintain the integrity of data, the CPC permits the authorities to require any person in possession or control of data to protect its integrity.

6.1.1.4 Rendering inaccessible or removing the computer data in the accessed computer system

The situation with regard to removing data or rendering them inaccessible is less clear. Very few Parties (for example Albania, Cabo Verde, Dominican Republic, Fiji, Mauritius, Philippines, Portugal, Senegal, Sierra Leone) have a specific statute granting this power. Most rely on an implicit power to meet this element of Article 19.3: if we seize data, then it is unavailable to the searched person or entity[58]. This approach means that the officials executing a seizure must ensure that they have removed the target data from every place where it is stored, not merely that they have removed one copy.

However, it should be noted that the power contained in Art. 19.3 captures both devices seized at the location (through Art. 19.3.a., e. g., seizing a domain server hosting an illicit website) and computer data deleted or rendered inaccessible from the location of an executed search warrant (through Art. 19.3.d., e.g., an illicit website rendered inaccessible by the authorities), as opposed to specifically ensuring a website is unreachable through engagement with other persons, such as through service providers.

There were insufficient answers for any conclusion about the ability to render data inaccessible without removing them. Some Parties (France, Netherlands) stated that they had the power to remove online data or render them inaccessible, for example, through notice and take-down or other means to make a website unreachable pursuant to a criminal investigation (for example in relation to cases of child sexual abuse of which materials were made and are disseminated). Article 19.3 does not specifically demand this power. This power is of increasing interest to Parties, for example in cases of child sexual abuse material.

Some Parties (for example Andorra, Austria, Brazil, Finland, Germany, Lithuania, Slovenia) have not adopted special provisions for disabling or removing computer data in an accessible computer system and rely on the use of the general provision of seizure or confiscation of objects provided by their framework that does not mention electronic search and seizure specifically.

[58] At least until the time when the authorities may be required to return the data pursuant to statute.

Several Parties pointed out that this power is also important in the context of the seizure of crypto currencies (Liechtenstein, Switzerland). One Party specified that it had adopted domestic guidelines in this regard (Georgia).

Examples of practices include:

- Belgium: Where it is not possible to copy the data stored, for technical reasons or because of the volume of the data, the Public Prosecutor shall use appropriate technical means to prevent access to such data in the computer system, as well as to copies of such data that are available to persons authorised to use the computer system. If the data are the subject of the offence or have been produced by the offence and if they are contrary to public policy or morality or constitute a danger to the integrity of computer systems or to data stored, processed or transmitted through such systems, the Public Prosecutor shall use all appropriate technical means to render the data inaccessible or, after taking a copy of them, to remove them.

- Finland: Relevant case law: A was convicted of aggravated distribution and possession of an indecent image of a child and was ordered to forfeit to the State the illegal video and image files stored on the hard disks of a laptop owned by A's spouse B and of an external hard disk drive owned by A. After deleting the files, the Court of Appeal ruled that the computer and the drive had to be returned to their owners. The prosecution demanded that the laptop and the external hard disk drive be confiscated or at least that the hard disk drive of B's computer be overwritten. On the grounds set out in the judgment of the Supreme Court, the laptop and the external hard disk drive were ordered to be forfeited to the State. The forfeiture order was ordered to lapse if, at the expense of the owner of the device, the illegal files were removed from the device either by removing and destroying the hard disk of the device or by overwriting all the files on the hard disk in a way that ensured their removal after the legal files had been copied according to the owner's instructions and returned to the owner.

- USA: The original media is usually seized and maintained in the possession of law enforcement, thus rendering the data inaccessible to the owner. In certain circumstances, particularly in the case of ongoing businesses, law enforcement will work with the owner of the data to create an identical copy of the data such that the business can continue to operate even after a warrant has been executed. Alternatively, the owner of data can seek return of the data from the government or petition the court for it return or for a copy.

6.1.1.5 Procedures when the location of data cannot be determined

This section of the questionnaire also included a question about applicable procedures when the location of data cannot be determined. Almost all of the Parties stated that they apply the same measures when extending a search (according to Article 19.2) and in situations when it cannot be determined where the data sought is stored.[59]

[59] Readers are advised to consult the previous Chapter of this report.

6.1.2 Competent authorities that authorise and carry out a seizure

Party	Competent authority that authorises a search	Competent authority that carries out a search
Albania	Judge	Prosecutor, Judicial police, expertise may be involved
Andorra	Investigating judge	Police officers and specialised authorities appointed by the investigating judge
Argentina	Judge	Prosecutors and police officers
Armenia	Judge	Investigators and technical experts
Australia	Magistrate, or a justice of the peace or other person employed in a court of a State or Territory who is authorised to issue search warrants or warrants for arrest	Law enforcement authorities including constables or constables assisting
Austria	Prosecution authority	Criminal investigation authority
Azerbaijan	Judge, Investigating judge	Law enforcement authorities with technical expert assistance
Belgium	39bis, § 2, paragraph 1: judicial police officer; 39bis, § 2, subparagraph 2: public prosecutor; 88ter : investigative judge; 90ter : investigative judge.	Police experts
Bosnia and Herzegovina	Judge	Prosecutors and police authorities assisted by computer forensics and digital forensics experts
Benin		
Brazil	Judge	Police officer with technical expert, prosecutor with technical expert, specialised units within police and prosecutorial services
Bulgaria	Judge	Investigator, an investigating police officer or an investigating customs officer. Other computer expert may be present
Cameroon	State counsel, examining magistrate	Police officer
Canada	Judge	Peace officer, public officer, technical expertise may be involved
Colombia	Judge	Judicial police
Costa Rica	Judge	Prosecutor's Office and/or the Judicial Police, specialised authorities
Croatia	Investigating judge, judge	Police officer and other specialised authority
Cyprus	Judge	Police officer
Czech Republic	Judge	Police officer
Denmark	Judge	Danish national police and other experts
Dominican Republic	Judge	Prosecutor, specialised cybercrime police
Estonia	Judge, prosecutor	Experts and other technical experts
Fiji	Judge	Police and technical experts

Party	Competent authority that authorises a search	Competent authority that carries out a search
Finland	Prosecutor, police officer	Police authorities and other technical experts
France	Judge, investigative judge, police officer	Prosecutor, police officer, deputy prosecutor. Qualified persons to carry out technical examinations
Georgia	Judge	Investigators with assistance of specialised investigators or other technical specialists from National Forensics Bureau
Germany	Judge	Police officer, prosecutor
Ghana	Judge, The Police, The Economic and Organised Crime Office (EOCO), The Office of the Special Prosecutor, National Security, National Investigation Bureau, The Judicial Service of Ghana	The Police, The Economic and Organised Crime Office (EOCO), The Office of the Special Prosecutor, National Security, National Investigation Bureau, The Judicial Service of Ghana
Greece	Judge, Prosecutor	Law enforcement agencies and their specialised units (Cyber Crime Division and Forensic Science Division in Greece)
Grenada	Magistrate, judge	Police officer (Digital Forensic Unit)
Hungary	Judge, prosecutor, investigating authority	Prosecutor, Police and National Tax- and Customs Authority as investigating authorities, consultants with specific expertise
Iceland	Judge, police officer	Police authorities
Israel	Judge	The National Police, the Tax Authority, the Military Police, the Department of Internal Police Investigations, the Securities Authority, the Competition Authority
Italy	Prosecutor	Police forces and other law enforcement agencies
Japan	Judge	Public prosecutors, public prosecutor's assistant officers or judicial police officials
Kiribati	Judge	Police officer
Latvia	Investigating judge	
Liechtenstein	Investigating judge	Digital Crime Unit of Liechtenstein’s National Police
Lithuania	Judge	pre-trial investigation officer or the prosecutor, IT specialists from Lithuanian Forensic Expertise Centre, the Criminal Investigation Centre or other law enforcement specialists
Luxembourg	Investigating judge, prosecutor	Police, technical experts
Malta	Magistrate	Police officers, technical experts
Mauritius	Judge	The police, The Independent Commission Against Corruption
Monaco	Judge, prosecutor, juge de libertes	State police (Cybercrime unit), IT experts

Party	Competent authority that authorises a search	Competent authority that carries out a search
Montenegro	Investigative judge	Police officers, officers of the Digital Forensic Centre
Morocco	Investigative judge (if the investigation is opened), prosecutor (during the investigation phase)	judicial police officer
Netherlands	Judge, prosecutor	Prosecutor and police officer
Nigeria	Judge	Police
North Macedonia	Judge	Prosecutor and law enforcement officer
Norway	Judge, prosecutor, police officer	Police (NCIS Norway/NC3), prosecutors and specialised personnel
Panama	Judge of guarantees	Prosecutor
Paraguay	Judge	Prosecutor
Peru	Judge	Prosecutor, National police
Philippines	Judge	Law enforcement officers
Poland	Judge, prosecutor	Police officer and other specialised experts
Portugal	Prosecutor	Police officer, specialised experts
Republic of Moldova	Investigating judge, prosecutor	Prosecutor, law enforcement officer
Romania	Judge	Police officer, prosecutor or a police officer investigating the case
San Marino	Judge	Police officer
Senegal	Investigating judge, prosecutor	Investigating judge; police under supervision of prosecutor or investigating judge
Serbia	Judge	Police
Sierra Leone	Judge	Law enforcement officer
Slovak Republic	Judge, prosecutor	Forensic technicians or experts
Slovenia	Judge	police officer
Spain	Judge	Prosecutor, police officer, forensic engineering laboratories
Sri Lanka	Magistrate	Police officers, CERT, court-appointed experts
Sweden	Investigation leader, prosecutor or judge	Investigating authority
Switzerland	Judge, prosecutor	Police officer, other specialised authority
Tonga	Magistrate	Police officers, CERT, foreign forensic experts
Tunisia		
Türkiye	Judge, prosecutor	Law enforcement units (with forensic expertise)
Ukraine	Investigating magistrate, judge	Investigator, prosecutor
United Kingdom	Magistrate	Police officer
United States of America	Judge	Law enforcement officer

6.2 Implementation of Article 19.3 – Assessment

Answers to the following questions were assessed:

- 2.3.1 Please summarise what legislative or other measures your country has undertaken to ensure that your authorities are able to seize or similarly secure computer data as described in Article 19.3. In answering, please summarise the requirements to be met and the procedural steps typically taken to obtain the authorisation for such a seizure.
- 2.3.2 Do you apply the same measures when extending a search (according to Article 19.2) and in situations when it cannot be determined where the data sought is stored?
- 2.3.3 Which are the competent authorities that authorise and that carry out a seizure as described in Article 19.3? What type of technical or other expertise is required and utilized?

Party	Legislative and other measures	Assessment
Albania	Albania indicated that, by Article 208/A of the CPC, it is the court that authorizes the public prosecutor to order the judicial police officer to exercise the powers referred to in Article 19.3. Albania also indicated that the same procedure and powers apply to the extension of a search, but there is no specific provision in the case of an undetermined location of computer data. Article 209/A of CPC establishes "…3. In executing the court decision, the prosecutor or the judicial police officer authorized by the prosecutor shall adopt measures: a) to prevent any further action being taken or to secure the computer system or part of it or of another data storage device; b) to take out and obtain copies of computer data; c) to prevent the access to computer data, or to remove such data from accessible computer systems; d) to ensure the inviolability of the relevant stored data. The competent authorities to authorize and carry out the seizure described in Article 19(3) are the public prosecutor or the judicial police officer if the public prosecutor decides so. As mentioned above, the public prosecutor may appoint an expert with knowledge of the functioning of computer data or protective measures for the protection of computer data.	Albania applies specific search and seizure powers to implement Article 19.3.
Andorra	Procedures with regard to Art. 19.3 are the same as previously described. Articles 26 and 87 of the criminal code meet certain elements of Art. 19.3 – seizing and securing systems and media, making and copying data, and maintaining the	Andorra applies general search and seizure powers to implement Article 19.3. Provisions specific to computer

Party	Legislative and other measures	Assessment
	integrity of evidence. Further, the judicial authorities have the power to render data inaccessible or remove them: an investigative judge can issue an order for police technical assistance to take whatever measures are necessary.	data and systems could permit greater clarity and enhance legal certainty.
Argentina	There is no express provision in force in the whole country that fulfils all the elements of Art 19.3. Argentina applies the principle of freedom of evidence. It is important to mention that the Federal Code of Criminal Procedure (CPPF), in Articles 151 and following, regulates the seizure of computer or electronic data: Art. 151 "the judge may order, at the request of a party and by a reasoned order, the search of a computer system or part thereof, or of a computer or electronic data storage medium, in order to seize the components of the system, obtain a copy or preserve data or elements of interest to the investigation." Implementation of that provision across the country is not complete and continues. The same limitations shall apply as those provided for the seizure of documents. The examination shall be made under the responsibility of the party that requested it. Once the components of the system have been seized, or a copy of the data has been obtained, the rules for the opening and examination of correspondence shall be applied. The return of the components that have no relation to the process will be ordered and the destruction of the copies of the data. The interested party may appeal to the judge to obtain the return of the components or the destruction of the data. Art. 153 regulates the procedure for the recording and preservation of the evidence that will be recorded by means of a tape recording or other similar technical means that ensure the fidelity of the record. The recording shall be delivered or kept by the representative of the Public Prosecutor's Office who shall provide for the corresponding security measures, applying the measures foreseen for seizure and chain of custody. The representative of the Public Prosecutor's Office shall ensure that it is not known by third parties. At the end of the proceedings by judgment or dismissal order, the sound recordings of the communications and the transcriptions that have been made shall be placed in safekeeping from public access. The latter may not be accessed, except by court order. Seizure or similar securing of data that have been accessed through extension of search is not provided for in the legislation.	Argentina has introduced specific search and seizure powers to implement Article 19.3. not yet applicable in the whole country. In the meantime, in practice Argentina applies a combination of general and specific search and seizure powers to implement Art. 19.3. More information could better clarify how specific elements, in particular under c-d of Art. 19.3 of the BC are applied. Specific provisions could permit greater clarity and legal certainty.

Party	Legislative and other measures	Assessment
Armenia	Armenia stated that it has put in place legislative and other measures to permit the authorities to seize or similarly secure a system or storage medium, to make and retain copies of data, maintain data integrity and remove data or render it inaccessible. Armenia refers to Art. 236 as the applicable legal basis for the implementation of all elements of Art. 19.3. However, while it appears that it meets some of the elements of Art. 19.3, it does not seem to address requirements of Art. 19.3.d of the BC. Similar measures and procedural steps are utilised when searches are extended under Article 19.2. Authorities may proceed only when it is possible to determine the data are stored in Armenian territory. Judicial authorities issue seizure authorisations if the evidence presented meets legal requirements. Law enforcement agencies execute the seizure and may employ forensic and other experts.	Armenia applies specific search and seizure powers to implement Article 19.3. However, it is not clear how this provision addresses requirements of Art. !9.3.d. of the BC. More specific provisions could permit greater clarity and enhance legal certainty.
Australia	Australia can satisfy the elements of Article 19.3 per numerous sections of the Crimes Act and SD Act and police force procedures. Computer-specific provisions expressly permit seizure of devices and data and copying of data. Police forces have procedures to maintain the integrity of data; in addition, the two statutes bar alteration of the data. As for removal of data or rendering them inaccessible, the Crimes Act provides that devices and computer files may be seized if their possession could constitute an offence. In such cases, the authorities do not have to give a copy of the item to the person concerned, as would be normal. Pursuant to a law or court order, return of the item can be barred and it can be retained by the authorities or disposed of. Under the SD Act, a "data disruption" warrant may be procured. It permits authorities to disrupt data to frustrate the commission of a covered offence. Australia applies the same measures in extending a search and in situations when the location of the data cannot be determined. In the same way as previously described, searches per Article 19.3 are authorised by a member of the judiciary and executed by a member of certain Australian law enforcement agencies.	Australia applies specific search and seizure powers to implement Art. 19.3.

Party	Legislative and other measures	Assessment
Austria	Section 111 of the Criminal Procedure Code sets out some of the regime for searches and seizures, including seizing and similarly securing data or systems and making a copy of data. A 2022 Decree, "Guideline for the handling of seized objects," addresses at length and in great detail the issues of copying, securing and maintaining the integrity of seized data. A section of the criminal code regarding seizures effectively provides for removal of data or rendering them inaccessible, while several sections of the Austrian Media Act explicitly provide for the same. The same measures apply to extended searches. In certain circumstances and subject to certain rules, extension of searches is possible even when not initially authorised. Seizures are authorised and executed as described above.	Austria applies a combination of general and specific search and seizure powers to implement Article 19.3.
Azerbaijan	There are no specific provisions regarding the elements of Article 19.3, but, in practice, the general provisions for evidence collection and preservation apply to fulfil the requirements of 19.3. Articles 245 and 251 of the CPC stipulate that, if possible, items that have been removed must be packaged, sealed and stored on the premises of the investigating authority or court, or handed over for safekeeping to a representative of the competent state authority, who must be warned of their legal liability, and that items that have been seized but not removed must be sealed and handed over for safekeeping to their owner or possessor or to adult members of their family, who must undertake not to misappropriate, damage or destroy them, and who must be warned of their legal liability. In this regard, the same measures are partially applied in the case of an extension of a search and in situations where the location of the data cannot be determined. The authorising and executing authorities are the same as in searches pursuant to Article 19.1.	Azerbaijan applies general search and seizure powers to implement Article 19.3. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.
Belgium	As Belgium details, several sections of the code provide for the elements of Article 19.3, including rendering data inaccessible in certain cases or removing it. These provisions also apply when searches are extended and it is not possible to determine the location of the data. The usual authorities are responsible for authorising and executing such seizures.	Belgium applies specific search and seizure powers to implement Article 19.3.
Bénin	Articles 589 and 590 of the digital code act spell out the required procedures and steps. They are the same as mentioned with regard to Article 19.2. The authorities competent to authorise a seizure per Article 19.3 are the juge d'instruction and the Prosecutor of the Republic. The judicial police execute the seizure using methods that preserve the physical integrity of the hardware and the integrity of the seized data. Technical expertise is provided either by the	Bénin applies specific search and seizure powers to implement Article 19.3.

Party	Legislative and other measures	Assessment
	Technical and Scientific Police or the Digital Investigation Lab of the National Center for Digital Investigation (Centre National d'Investigations Numériques (CNIN)).	
Bosnia and Herzegovina	The different codes in force in the country have diverse approaches to this particular paragraph of the Budapest Convention. The code of Bosnia and Herzegovina has not implemented legislation related to the elements of Article 19.3. The CPC of the Federation Bosnia and Herzegovina provides for the different manners of seizing of data, as described in Article 19.3. The CPC of Republika Srpska only seems to provide for searching by the means of making a copy of computer data (Article 19.3.b). When sufficient grounds exist to suspect that there is evidence of a criminal offence on temporarily confiscated electronic devices, a court may issue an order for the creation of a forensic copy. The forensic copy will be created by specially-trained authorised officials or by another expert in the presence of an authorised official. Those officials will report on its creation, describing and identifying the item exactly. The seized item and copy are then held for safekeeping by the court or under its supervision. The CPC in Brcko District does not include the elements of Article 19.3. However, it was reported that, in practice, some of the forms of seizure of this paragraph occur. It is namely the case of a (seizing data), c (maintain the integrity of the data) and d (in the modality of deleting data). The elements of Article 19.3a are implemented by temporarily confiscating cases based on a court order or by obtaining data from ISP/OSP based on a court order, which is prescribed in the CPC BD BiH. In practice, on the basis of a court order, part or all of a searched system is temporarily confiscated. After that, the authorities request an order permitting the confiscated item to be searched. The elements of Article 19.3b are implemented by having them included in the court order for the search. In the application for the warrant, the police will request that the order authorise the creation of a forensic copy to be retained	Bosnia and Herzegovina applies a combination of general and specific search and seizure powers to implement Article 19.3. It appears that several elements of Art. 19.3 were not implemented into the domestic law of Bosnia and Herzegovina. Provisions specific to computer data and systems applicable to all entities of Bosnia and Herzegovina could permit greater clarity and enhance legal certainty

Party	Legislative and other measures	Assessment
	in addition to the original device that is the subject of the search searches and a forensic image of the memory space of the device. In most cases, the court will issue an order with such elements. As to Article 19.3c, in practice, if the data are in the possession of an ISP, the police will submit a request for the ISP to store the data. Such storage is voluntary. If the data are in the possession of the authorities due to a search, standard best practices in digital forensics are applied to ensure the integrity of the stored computer data and to record any unavoidable data changes. As to Article 19.3d, the criminal code (in particular Articles 78 and 391) authorises confiscations in numerous circumstances. These include when confiscation is required by the interests of general security and morality and when items were involved in the commission of a crime, notably damage to computer data or programs or computer forgery and exploitation of minors for pornography or introducing minors to it. There are no specific rules respecting seizure of data in cases of extension of searches. However, it was reported that the general rules and principles on seizure of data would apply, when extending searches, including in cases of "lost of location". That is, Bosnia and Herzegovina, the Federation Bosnia and Herzegovina, and Republika Srpska may seize data in an unknown location in the same way as they extend searches. Regarding the competent authorities, prosecutors (and, in Republika Srpska, authorised officials with prosecutorial permission) obtain authorisation for searches and seizures from courts. Police and technical experts carry out the order.	
Brazil	The authorities stated that the text of Art. 19.3 of the Budapest Convention directly applies as domestic legislation, while the general domestic law does not explicitly provide for data seizure measures. The general provisions of the Code of Criminal Procedure apply by analogy and competent authorities have the power to seize or secure computer data that have been searched or similarly accessed. This includes the seizure of computer hardware and data storage media. In this context, "seize" is interpreted similarly to the definition provided in the Convention. It means to remove the physical medium in which the data are recorded or to make and retain a copy of such data. It also includes the seizure of programs needed to access the data. Furthermore, the term "similarly secure" is recognized to reflect other means by which data are removed or their control is taken over. Regarding 19.3.d, the practice of making data inaccessible, whether through encryption or other technological measures, requires judicial authorisation. The term "removal" is	Brazil applies general search and seizure powers to implement Article 19.3. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.

Party	Legislative and other measures	Assessment
	interpreted in the sense that the data are removed or made inaccessible, but not destroyed. The seizure does not imply the final deletion of the seized data. The Competent authorities must have a court order or search warrant based on reasonable suspicion of an offence, specifying the location, type of data, and time frame for the seizure. The seizure process must preserve the integrity of the data and any copies made should be kept securely. Brazil ensures compliance with the measures described in Article 19.3 of the Budapest Convention by maintaining the chain of custody, as specified in the Code of Criminal Procedure. The chain of custody includes several steps, including the identification, isolation, fixation, collection, packaging, transport, receipt, processing, storage, and disposal of the evidence. Article 158-C of The Code of Criminal Procedure emphasizes that the collection of evidence should preferably be carried out by an official expert who will carry out the necessary procedures for custody, even in cases where additional examinations are required. In order to carry out a seizure under Article 19.3, competent authorities, which are typically law enforcement agencies (such as federal police, state police or other specialized units responsible for investigating cybercrime and related offences), will normally require a court order or search warrant authorising the seizure, based on reasonable suspicion of the commission of an offence, and specifying the location of the computer data, the type of data to be seized and the time frame for the seizure. They may also require the assistance of technical experts, such as computer forensic specialists or digital evidence analysts, to assist in the seizure and analysis of the computer data.	
Bulgaria	During a search, the investigative authorities have the power to seize any object (including an information system), which they believe contains evidence relevant to the crime under investigation. According to the practice, during a search the preferred option is to take the computer data storage medium. If this would be difficult, a forensic copy could be made in the presence of a computer expert and handed over to the authority, which carries out the search. Seizure must be authorised by a judge. Concerning the specific elements of 19.3:	Bulgaria applies specific seizure powers to implement Article 19.3. It is not clear, however, that Bulgaria has the power to remove content or render it inaccessible if it is not in the hands of a service provider – if it is stored by a business, for example.

Party	Legislative and other measures	Assessment
	a) Seizure of the relevant means of storage is the preferred method and most often used by law-enforcement to secure computer data for an investigation. b) A copy of the computer data is done in cases where the seizure of the computer data is not an option (e.g. where a hosting provider hosts several virtual computer systems on a single hard drive). The process is described in the protocol for the search and seizure or the copy is prepared in the presence of the investigator and handed over with a separate protocol to the law enforcement authorities. c) The integrity of computer data is maintained either by seizing it or by making a copy. It appears that Article 163 of the CPC may also be applicable. It provides in detail for the sealing of seized computer storage media, for detailed physical records of the sealing, and for special procedures for unsealing the data carrier to further the investigation. d) Under Article 16(2)of the law on electronic trade, hosting providers must render content inaccessible if the provider has been informed by law enforcement that the content is illegal. (Providers have a separate obligation to remove content or render it inaccessible if they themselves realise that content is illegal)	
Cabo Verde	According to Article 18 of the CL, the competent judicial authority, which in Cape Verdean Legal Order includes Judges and Public Prosecutor's Office magistrates, may authorize or order the seizure of computer data during a computer search. If such an order or authorization exists, the seizure must take the following forms: i) Seizure of the support where the system is installed or seizure of the support where the computer data is stored, as well as the devices necessary for reading it. ii) Making a copy of the data, on an autonomous medium, which will be attached to the process; iii) Preservation, by technological means, of data integrity, without copying or removing them; or iv) non-reversible deletion or blocking of access to data. At least in the case of paragraph v), the copy is made in duplicate, one of the copies being sealed and entrusted to the judicial secretary of the services where the process takes place and, if this is technically possible, the seized data is certified by digital signature means. The Public Prosecutor's Office will ask the judge for permission to seize. If it is a Criminal Police body, it will always send a request to the Public Prosecutor's Office. The Public Prosecutor's Office will authorize or request authorization from the judge if it is no longer within its competence, as previously mentioned. If the Police carry out a seizure outside of authorized or prior order cases, they must submit the seizure to the competent judicial authority for validation within 72 hours.	Cabo Verde applies specific search and seizure powers to implement Article 19.3.

Party	Legislative and other measures	Assessment
	It is the same measures as when extending a search, which is the general regime for seizing computer data, regardless of how they are obtained. The law does not address situations where it is impossible to determine the location of the requested data. However, this scenario has not yet arisen in practice. In any case, the first obligation of anyone conducting a computer search is to determine the specific location of the data. In Cabo Verde, the Judge or Public Prosecutor's Office, as the competent judicial authority, may authorize or order the seizure of computer data following Article 18 of the CL. Cape Verdean law includes a provision that requires any seized data or computer documents likely to reveal personal or intimate information that could compromise the privacy of the holder or a third party to be presented to the judge. Failure to do so will result in nullity. The judge will then consider adding the data or documents to the process, considering the interests of the specific case. The criminal police bodies, that is, are the entities that carry out the physical seizure of data, and may, without prior authorization from the judicial authority, carry out this seizure during a computer search legitimately ordered and executed, as well as when there is urgency or danger in delay. Regarding the necessary technical knowledge, the law does not make any special requirements.	
Cameroon	Article 29 of Cameroon's cybercrime law expressly empowers the authorities to seize the installations of information systems of operators by order or with a warrant issued by judicial authorities. Searches and seizures are subject to compliance with the conditions set out in the CPC. The state counsel or the competent court authorises searches and seizures. Police forces execute them in collaboration with technical institutions such as the National Agency for Information and Communication Technologies (ANTIC). Procedures have not yet been clearly established for handling situations when the location of data cannot be determined.	Cameroon applies a combination of general and specific search and seizure powers to implement Article 19.3. However, it is not clear how the powers to make and retain a copy of data, maintain the integrity of data, and remove data or render it inaccessible per Article 19.3 b-d are implemented in Cameroon.
Canada	Section 487 of the Criminal Code and subparts address searching, seizing and copying data. With respect to implementation of Art. 19.3.c., in a very detailed reply, Canada refers to Art. 490 of the Criminal Code as the applicable provision. The provision provides for a general power regulating the procedure of perishable things, including their return to the lawful owner or other persons lawfully entitled to their possession. Furthermore, the relevant domestic legislation for the implementation of Art. 19.3.c. can be found in sections 31.1 to 31.8 of the Canada Evidence Act (CEA) which relate to computer data / electronic documents (Authentication of electronic documents, best evidence rule). Canada	Canada applies a combination of general and specific search and seizure powers to implement Article 19.3.

Party	Legislative and other measures	Assessment
	also submitted court decisions that provide overview of the applicable legal framework related to maintaining integrity of data. It was also highlighted that a mandatory set of courses must be successfully completed by a law enforcement member through the Technological Crime Learning Institute at the Canadian Police College to help ensure the consistency of forensic practices across Canada. Several articles under Criminal Code provide for implementation of Art. 19.3.d. This includes also Section 487.01 that provides for a warrant that can authorize the use of any device or investigative technique or procedure or do anything described in the warrant that would, if not authorized, constitute an unreasonable search or seizure in respect of a person or a person's property and can address the requirements of 19.3.d. The same measures are applied in situations when the location of the data cannot be determined as when searches are extended per Article 19.2. As previously described, seizures are authorised by judges. Seizures are executed by peace officers (or possibly by public officers). Officers with special technical expertise may be involved.	
Chile	Chile does not have an express provision regarding seize of computer data and media containing computer data. It appears that in practice, provisions of the Code of Criminal Procedure regarding seize of physical evidence may probably be used by analogy. General powers provided for in Art. 217 of the CPC that regulate seizure of objects and documents may be used. The authorisation is granted through a court order issued at the request of the prosecutor.	Chile applies general search and seizure powers to implement Article 19.3. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.
Colombia	Article 236 of Law 906 of 2004 allows digital evidence to be obtained to be secured and copied while maintaining its integrity by established forensic standards. For this purpose, several fundamental aspects must be verified: 1. The Access to the device; place where the device that stores or contains the data is located: During this first phase, the Judicial Police, and the Prosecutor in charge of the investigation must issue orders within the case that allow access to the place or device where the data is stored. i) Access to digital evidence found in the framework of an arrest procedure. ii) Access to the physical space where the device is located through the development of searches and seizures. iii) Access to the device using a personal register. iv) Access to the space or device with the victim's consent.	Colombia applies general search and seizure powers and jurisprudence and accepted practices and chain of custody manuals to implement Article 19.3. Provisions specific to computer data and systems are recommended to permit greater clarity and enhance legal certainty.

Party	Legislative and other measures	Assessment
	2. Access to the data stored in the seized devices; Once the seizure of the device has been exhausted, the Prosecutor may order the extraction of the stored data with the support of a Computer Forensic Expert, the data extraction process must be documented in an expert report, detailing the scientific and technical methods employed, the efficacy of tools used for forensic analysis, the specific process applied to evidence including unpacking and analysis, and the expert's conclusions upon completion of the analysis. 3. Access to data where seizure of the item is not possible; There are cases where the size of the item, its connection to more complex systems, or practicality does not allow the physical seizure of the item. In these cases, the Prosecutor will enter the space where the system is located with the authorization of the owner of the site or with a search warrant and will order the preservation of the digital evidence, by the provisions of Article 236 of the CPP. 4. The act of making the data inaccessible or removing it from the system from which it was recovered; There is no direct rule that considers this specific action. However, the Manual of Chain of Custody and Judicial Police of the Attorney General Office confers within its functions to the forensic experts so that, within the process of identification and extraction of data stored within a computer system, they can change and take control of users and credentials that can be used for the elimination or modification of digital evidence. Colombia added another commonly used mechanism to suspend public access to specific content or the deletion of data after it has been retained using the figure of "reestablishment of the right of victims" contained in Article 22 of the Colombian code of criminal procedure. Under this measure, a prosecutor may request a precautionary measure from a judge of the republic, any action, including the deletion, suspension of access or any other measure considered relevant to a piece of data, to avoid the effects of a crime or to reverse the consequences of a crime within the framework of victim protection. This action has been used successfully to disable domains with pornographic content, remove offensive or illegal content on third-party systems, or suspend access to certain data by the suspect.	
Costa Rica	Costa Rica referred that there is no specific legislation regulating the search or seizure of stored computer data, but the Law regulating search, Seizure, and Examination of Private Documents and Intervention of Communications is applied. It is important to note that the authorities mentioned that this law explicitly equates digital evidence with physical or documentary evidence. According to the same, after the electronic device has been seized or the database containing the digital evidence of interest has been located, it is required to obtain judicial oversight for its acquisition. Once	Costa Rica applies general search and seizure powers to implement Article 19.3. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.

Party	Legislative and other measures	Assessment
	granted, it will be the responsibility of the technical police to carry out forensic procedures for obtaining (backing up) and analysing the information, all of which will be documented in a report presented to the legal proceedings. The seizure of hardware with electronic data can be ordered by the prosecutor or Judicial Police to protect the evidence, but searching and analysing the data requires a judge's order due to the owner's right to privacy. If you can´t determine if the data are in Costa Rica territory, and the provider of the service has no open office in our country, the judge will not extend the search, so we must rely of international cooperation.	
Croatia	Articles 261 and 263 of the CPC provide specifically for the seizure of electronic devices and data and for their safekeeping. Data are removed or rendered inaccessible via the investigating judge's ruling; normally, they will be returned no later than six months from the date of seizure, but return may be barred for several reasons relating to criminal offences. Article 262 of the CPC protects certain items from seizure. In general, these protections relate to items held by privileged classes of persons – for example, defence counsel and journalists – and to secret government documents. The protections may be lifted if a person in a privileged class is suspected of criminal complicity. The measures are applied regardless of the location of data.	Croatia applies specific search and seizure powers to implement Article 19.3.
Cyprus	Even in the absence of a specific law allowing it, it seems that, in practice, the four modalities of seizure, described in Article 19.3, can be executed, by specific mention in the judge's order that decides it. It seems that all of them are foreseen in an internal manual of procedures, used by police. The Digital Forensic Lab (DFL) of the Cyber Crime Unit is responsible for seizing or similarly securing a computer system or part of it or storage media. It is also responsible for making and retaining copies of the data, maintaining their integrity, and removing data or rendering them inaccessible.	Cyprus applies general search and seizure powers to implement Article 19.3. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.
Czech Republic	The measures concerned include provisions on Obligation to Handover or Surrender Items (Provision 78) and Removal of Items from Possession (Provision 79) both defined in the Criminal Procedure Code (CPC).	Czech Republic applies general search and seizure powers to implement Article 19.3. More clarification how the framework applies to making copies of

Party	Legislative and other measures	Assessment
	When it comes to maintaining the integrity of the relevant stored computer data, internal standard operating procedures are used. The call to handover or surrender an item may be made by the presiding judge and in pre-trial proceedings by the public prosecutor or police authority. If the item is not handed or surrendered voluntarily, such an item may be removed from possession upon an order of the presiding judge an in pre-trial proceedings upon an order of the public prosecutor or police authority. The police authority must have a previous consent of the public prosecutor for issuing such an order; without such consent the police authority may issue such consent only if the previous consent cannot be secured and the matter cannot be delayed. If the authority that issued the order does not perform the removal of the item from possession by itself, it will be performed by the police authority on the basis of the order. Since it is relied on application of general powers, more clarification how the framework applies to making copies of data and removal of data in particular would be desirable. Alternatively, it is also possible to apply the order to preserve data or the order to deny the access to it according to provision 7b of the CPC. The authorities apply the same measures when extending a search and in situations when it cannot be determined where the data sought are stored.	data and removal of data in particular would be desirable. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.
Denmark	The responses did not directly address elements a through d of Article 19.3. Searches and seizures are extensively regulated by the AJA. Under Section 802, computer data are covered by the word "objects," and that section lays out the conditions of the seizure of a person suspected of a crime. Thus the usual rules and procedures are employed and the usual officials are involved in the seizure of data. The responses indicated that the usual rules and procedures are employed, and the usual officials are involved, when searches are extended and when the location of data cannot be determined.	It appears that Denmark applies general search and seizure powers to implement Article 19.3. More information regarding implementation of specific elements of Article 19.3 may be desirable. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.

Party	Legislative and other measures	Assessment
Dominican Republic	The Dominican Republic legislation establishes that, before obtaining a judicial order, the Public Ministry, with the assistance of state investigation agencies, has the power to i) Seize or secure an information system or any of its components, in whole or in part; ii) Make and retain copies of the content of the information system or any of its components; d) Order the maintenance of the integrity of the content of an information system or any of its components; e) Collect or record data from an information system or any of its components through the application of technological measures (art. 54) The Dominican Republic legislation makes no difference in respect to apply the same measures when extending a search, so the same measures apply. In Dominican Republic legislation, the competent authority that authorizes the order is a judge. The seizure is carried out by the Public Ministry assisted by officers from specialized cybercrime police units. These officers must belong to one of the specialized agencies, which have the technical expertise to properly carry out the digital evidence chain of custody process.	Dominican Republic applies specific search and seizure powers to implement Article 19.3.
Estonia	There are no specific provisions in the CPC regarding collection of computer data. Generic law enforcement powers are used (for example, powers under CPC Article 215) as well as generic powers of search and seizure (CPC Article 91). For the examination of objects (computer systems, data carriers, etc), CPC Articles 86 and 87 are used (inspection of document, another object or an item of physical evidence and report of an inspection, respectively). Beyond the relevant CPC articles, the police utilise internal, non-public guidelines on the collection and handling of electronic evidence. Depending on the case and needs, a forensic copy is made of the data carrier or objects are seized and examined later. Same provisions and principles as when extending a search are applied. Search and seizure can be authorised by the Prosecutor's Office as a rule. Certain exceptions are in place with regard to lawyers and notaries.	Estonia applies general search and seizure powers to implement Article 19.3. It seems that Estonia does not have the power to remove data or render them inaccessible. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.
Fiji	Both articles 16 and 21(3)(4) of the TCA provide legal basis for this measure. So, the Police/FICAC may apply for a warrant to a Judge/ Magistrate to seize the computer system or any part therein, computer data storage medium, make and retain a copy of computer data by using on-site equipment, maintain the integrity of the relevant stored computer data, render inaccessible or remove computer data in the accessed computer system, take a printout of output of computer data, secure computer system/computer data storage medium or part of it.	Fiji applies specific search and seizure powers to implement Article 19.3.

Party	Legislative and other measures	Assessment
	Authorities reported that they apply the same measures when extending a search, but not in situations where it is not possible to determine when the data sought was stored. The competent authority to authorize the seizure is judge, and those who carry out the search are the police and officials with technical expertise.	
Finland	There is no provision specifically regulating the powers of Art. 19.3. Rather, Finland uses the provisions generally provided for the seizure of physical items to implement Art. 19.3. According to the CMA, objects, property, or documents may be seized if there are reasonable grounds to suspect that they are relevant as evidence are involved in a criminal offence or are liable to be confiscated. This also applies to information contained in technical devices or information systems. The provisions in the Coercive Measures Act Chapter 7 regarding a document apply also to a document that is in the form of data. These provisions include the power of seizure of computer hardware, computer data storage media and the data carrier. Section 3 sets out rules on the prohibition of seizure and copying concerning close persons and the right to silence. Section 13 concerns the management of a seized object. The person carrying out the seizure shall take possession of the seized object, property, and document, or place it in secure custody. There is no explicit provision in law stating the requirement to maintain the integrity of the relevant stored computer data. However, according to the Coercive Measures Act, Chapter 7, Section 13, paragraph 3, the object of the seizure must be preserved in its original state and managed with care, and this requirement also applies to data. Additionally, the Coercive Measures Act, Chapter 8, Sections 24 to 26, provides provisions for data preservation orders that ensure the integrity of the data before copying or seizing the devices. Concerning rendering inaccessible or removing those computer data in the accessed computer system, the authorities informed that The CMA Chapter 7 permits data seizure even if it can be ordered forfeited. In cases of illegal content, the copying of data is not sufficient measure and allows rendering the content (Penal Code Chapter 10 section 5 paragraph 1.).	Finland applies general search and seizure powers to implement Article 19.3. that are extended by the domestic law to cover also computer data.

Party	Legislative and other measures	Assessment
	The object of the seizure may be left with the person who had it in his or her possession unless this would endanger the purpose of the seizure. The object of the seizure shall be preserved as such, and it shall be managed with care. Tests may be taken on an object seized for evidentiary purposes if these are necessary to clarify the offence. Finland applies the same measures when extending a search when it cannot be determined where the data sought are stored. The location of the data does not, as such, affect the decision-making on the coercive measure. If the location is unknown, special care will be exercised in the matter and, where possible, an express judicial consideration carried out before taking the measure. If mutual assistance must be requested, the rules of international judicial cooperation will be followed.	
France	Several articles of the CPC provide for satisfying the elements of Article 19.3. In particular, with regard to Article 19.3d, a judicial authority can request the closure of a website or remove access to the data hosted on a website (after having it seized for analysis and investigations). In the Bitzlato case, the judicial authority obtained the closure of the French site of this Virtual Assets Service Provider (VASP) that was prosecuted for illegal activities. Within the limits described above, the usual procedures are followed when the location of data is unknown. Police officials conduct searches. In cases that are at the preliminary investigation stage or where a juge d'instruction is already engaged, judges' orders will guide the searches.	France applies specific search and seizure powers to implement Article 19.3.
Georgia	General provisions of the CPC on physical seizure together with disclosure of computer data powers are applied. The powers concerned are subject to judicial authorisation. Usually, search and seizure are authorised through the same process and in the same warrant. Several articles of the CPC, including Article 136 specifically on computer searches, together provide for all the elements of Article 19.3. Authorities apply same measures as when extending a search. The powers are executed by law enforcement officers.	Georgia applies a combination of general and specific search and seizure powers to implement Article 19.3.
Germany	The general provisions of the Code of Criminal Procedure relating to objects that may be of significance as evidence for the investigation apply mutatis mutandis to data stored on a data carrier, which must generally be treated in the same	Germany applies general search and seizure powers to implement Article

Party	Legislative and other measures	Assessment
	way as other seized items. If the data are in the custody of a known person and is not surrendered voluntarily, the data must be formally seized in accordance with Section 94 (2) of the Code of Criminal Procedure. Pursuant to Section 98 (1) of the Criminal Procedure Code, seizures may only be ordered by the court, and in cases of imminent danger, they may also be ordered by the public prosecutor's office and its investigators. According to Section 110 (3) sentence 2 of the Code of Criminal Procedure seizure is also permitted on the extension of searches (according to Article 19.2) and in situations when it cannot be determined where the data sought are stored. If data are stored in a system that cannot be copied, data carriers can be seized (if in compliance with the principal of proportionality). The seizure and analysis of data are executed by specialists, which ensures the integrity of the data (see the comments on 2.4.1). If confiscated data contain incriminating material, it is not returned to the person in whose possession it was but deleted within the general deletion periods. There is no express reference to the provision or practices under domestic law for rendering inaccessible or removing computer data in the accessed computer system (19.3.d of the Convention).	19.3. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty. Clarification regarding implementation of Art. 19.3d would be desirable.
Ghana	Pursuant to the ETA, a law enforcement officer may seize any computer, electronic record, program, information, document or thing in executing a warrant under the Act (presuming that reasonable grounds exist to do so). An authorised person may assist the officer. The officer may access decryption information necessary to decrypt a record required for the investigation. The officer may make and take away a copy of any record or program held in the computer or in any other computer believed to contain evidence of another offence. Proper documentation and maintenance of the chain of custody for seized data is required. Depending on the circumstances and applicable laws, persons or entities affected by the seizure may be notified. Normally, a search and seizure is authorised by the judiciary. However, five prosecutorial, security and law enforcement agencies can authorise and execute searches and seizures in appropriate circumstances. It should be noted that the search and seizure provisions of the ETA may be used in addition to the powers of arrest, search and seizure of a law enforcement agency provided by other statutes. As fully described in the responses, procedures under the CSA (and the authorities involved) are similar, particularly in the elements of reasonable grounds for the seizure and numerous protective procedural requirements.	Ghana applies a combination of general and specific search and seizure powers to implement Article 19.3. Clarification regarding implementation of Art. 19.3.d. would be desirable.

Party	Legislative and other measures	Assessment
	The same measures are applied when searches are extended (as in Article 19.2) and in situations when the location of the data cannot be determined.	
Greece	Legislation provides for seizures (using the processes described above) that entail the powers to secure data, copy and retain it and maintain its integrity, and remove data or render it inaccessible. The same measures are applied when the location of data cannot be determined as when searches are extended. The competent authorities and experts involved are the same. Greece has a Cyber Crime Division and a Forensic Science Division.	Greece applies a combination of general and specific search and seizure powers to implement Article 19.3.
Grenada	Grenada informed that based on available/gathered information: 1. The investigator establishes the need for investigations 2. An affidavit of circumstances is presented to the magistrate 3. Search warrant is granted based on parameters and claims made in the affidavit 4. Search warrant is executed on the target/suspect The law regulates the removal of the system from its original place and not for the copying of data. Rendering the data inaccessible or removing content on the computer system is only as applicable in cases of violation of privacy or child pornography (in this act), covered under Section 32 (2). Grenada does not apply the same measures when extending a search and in situations when it cannot be determined where the data sought is stored. Seizure of the data may be authorised by a magistrate or a judge and executed by the Digital Forensic Unit. Local service provider/telecommunications company may be required to provide technical assistance.	Grenada applies specific powers to implement Art. 19.3. However, it appears that Art. 19.3.b of the BC has not been implemented while the domestic law implementing Art. 19.3.d has a narrower scope than required by the BC. Provisions more specific to computer data and systems could permit greater clarity and enhance legal certainty.
Hungary	Section 315 of the CPC covers all of the elements of Article 19.3.	Hungary applies specific search and seizure powers to implement Article 19.3.

Party	Legislative and other measures	Assessment
	Orders for seizure may be issued by a court, the prosecution service, or the head of the investigative authority concerned. The same procedures are followed when the location of the data is unknowns as when searches are extended. Orders for additional searches may be procured and the urgency of the situation may be taken into account. Seizures are executed by the police or another national law enforcement entity or the prosecution service. They have specially-trained personnel but may employ expert consultants.	
Iceland	The general provision on a seizure of items can be found in Art. 68.1 of the CCP. Art. 68.2 contains a rule of proportionality. As stated in the explanatory report to the respective provisions a less intrusive ways may be used to secure evidence. For example, the police may direct the owner or custodian to grant access to potential evidence, so that it can be viewed and photographed for the sake of investigation. Also, to provide information that an item contains, e.g. by delivering a photocopy or other form of a copy of a document or copies of electronic information from a computer. This milder remedy would include, among other things, being used when searching company premises instead of seizing, and thereby removing, original documents and computers found there. Article 69 of the CCP states that the police may seize items without a court order. However, there is a disclaimer in the second paragraph, which states that if items are in the keeping of a person other than the accused, and there is no danger that they will be destroyed or disposed of, seizure shall be decided by court order unless the unequivocal consent of the owner or keeper has been given. However, as stipulated by the Supreme Court of Iceland, although it is permissible to seize an object without a court order, cf. Art. 69.1 of CCP, Art. 68 of the same Code shall not be interpreted in such a way that the police can investigate the material content of electronic devices without a court order. In practice the police authorities in most cases make a copy of the seized documents. The integrity of the relevant stored computer data is maintained with the seizure of the data. A chain of custody is usually implemented with search and seizure reports and then recall reports on the handling of items. The police in general renders data inaccessible by seizing the computer or the object they are stored on.	Iceland applies a combination of general and specific search and seizure powers to implement Article 19.3. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.

Party	Legislative and other measures	Assessment
	Furthermore, Regulation no. 880/2019 on the handling, custody, and sale of seized, suspended and confiscated property and items. Article 20 of the regulation contains provisions on the handling and registration of electronic data which appears to contain some elements of Art. 19.3 of the Convention.	
Israel	Procedures relating to Article 19.3 are the same as described above, including when searches are extended or when the data's location cannot be determined. The legal framework authorises the seizure of data. In practice, in most cases, competent authorities seize the physical device upon which the computer data are stored, and later, using forensic tools, create a forensic copy of the computer data stored. In cases of computer data stored outside of Israel, competent authorities seize the device from which the data can be accessed, and then "seize" the data by creating a copy. Occasionally, seizure of computer data is done by way removal of the data, in cases where the device upon which the data are stored was not seized or was seized and then returned to the owner. Under Article 39 of the Criminal Procedure Ordinance, after a criminal conviction, the court may order the forfeiture, including the destruction of a seized item that was used to commit a crime. This can include the destruction of computer data.	Israel applies specific search and seizure powers to implement Article 19.3.
Italy	The Italian Criminal Procedure Code includes Article 254-bis, which outlines the seizure of IT data from IT, telematic, and telecommunications service providers. This article allows the judicial authority to order the seizure of data retained by these providers, such as traffic or location data. It permits the acquisition of this data by copying it into a suitable medium, ensuring its conformity to the original data and preventing any modifications. Service providers are also instructed to preserve the original data securely. In practice, the seizure can be executed by instructing the IT space administrator to take data offline, prohibit further access, change access credentials, or create a forensic copy of stored data. However, the provision does not seem to encompass all the situations foreseen by Art. 19.3. Italy indicated that it applies the same measures when conducting searches, including in cases where it is uncertain where the sought-after data is located. According to art. 252, the judicial authority orders the seizure of all other type of data (found during a search) stored in a computer or telematic system.	Italy applies general search and seizure powers to implement Article 19.3. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty, in particular as regards copying (Article 19(3)(b)) and deletion of data or making it inaccessible (Article 19(3)(d)) in cases where the data accessed by authorities pursuant to paragraphs 1 and 2 are not on the premises of the service providers.

Party	Legislative and other measures	Assessment
Japan	Several articles (largely described above) in the CPC combine to permit Japan to meet all the elements of Article 19.3 a through d. In general, the same considerations – particularly the facts of the individual case - are evaluated when a search is extended and when the location of the data cannot be determined. The same officials are involved at the same stages.	Japan applies a combination of general and specific search and seizure powers to implement Article 19.3.
Kiribati	The Cybercrime Act provides for seizures of computer data using the procedures described above. Seizures are authorised by a court and executed by the police, possibly with technical assistance. Law enforcement in Kiribati tends to stop at the stage when data location cannot be determined rather than extend a search.	Kiribati applies specific search and seizure powers to implement Article 19.3. However, it is not clear how the powers to maintain the integrity of data, and remove data or render it inaccessible per Article 19.3 c-d are implemented in Kiribati. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.
Latvia	Latvia can seize and search data and systems. Articles 191 and 192 of the CPC satisfy the requirement that Parties be able to make and retain copies of data and maintain its integrity. The data may remain in non-state custody, but it is subject to the strictures of Article 191 – for example, that the data be kept in an unchanged state for the period necessary for the needs of the proceedings. Latvia has the power to remove data. Under Article 219 of the CPC, Latvia seems to have all of the powers required by Budapest Article 19.3.	Latvia applies a combination of general and specific search and seizure powers to implement Article 19.3.
Liechtenstein	Two sections of the CPC provide for some of the requirements of Article 19.3. To maintain the integrity of the seized computer data, the number of files seized and the total storage size are compared directly after the copying process. If a court orders that data be made inaccessible, an entire device or system will be seized by the National Police. Data are not deleted during house searches.	Liechtenstein applies a combination of general and specific search and seizure powers to implement Article 19.3.

Party	Legislative and other measures	Assessment
	As noted, the same measures are applied when the location of data is unknown as when a search is extended – that is, Liechtenstein may carry out such searches if access to the data is possible from Liechtenstein. Warrants issued by a court after application by a prosecutor are executed by the Digital Crime Unit of the National Police. This unit has the expertise and resources for conducting IT forensics, including, for example, official wallets for the seizure of cryptocurrencies.	
Lithuania	Articles 94, 145, 147, and 155 (and 158 in cases of covert access) of the CPC fulfill the several requirements of Article 19.3. The actions involved may be authorised by a prosecutor but frequently must be authorised by a court. The same requirements are followed when the location of the data is not known as when a search is extended. Searches and seizures are authorised by a court after application by a prosecutor. The order is executed by the pretrial investigating officer or prosecutor. Examination of the data is done by specially educated and -equipped law enforcement personnel. IT specialists may assist.	Lithuania applies general search and seizure powers to implement Article 19.3. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.
Luxembourg	The procedures utilised to seize or similarly secure data under Article 19.3 are the same as those previously described. The provisions in Articles 33 and 66 of the CPC (supplied by Luxembourg) explicitly cover all four elements of Article 19.3. The same measures are applied when a search is extended as when the location of the data cannot be determined, as long as the data's storage medium may be accessed from within the physical territory. Specialised police carry out seizures of electronic evidence and call-in additional equipment and personnel as necessary.	Luxembourg applies a combination of general and specific search and seizure powers to implement Article 19.3.
Malta	The procedures described above are also used with regard to the requirements of Article 19.3: magistrates authorise seizures and the police (and possibly technical experts) execute them. The same measures are used when the location of the data cannot be determined. Pursuant to Chapter 9 Article 355L of the Criminal Code – '*The Police have the power to enter and search any premises, house, building or enclosure used, occupied or controlled, even temporarily, by a person who is under arrest, if they have reasonable grounds for suspecting that there is evidence, other than items subject to legal privilege, that relates*	Malta applies a combination of general and specific search and seizure powers to implement Art. 19.3.

Party	Legislative and other measures	Assessment
	to the offence or a connected offence, and such search shall be limited to the extent that is reasonably necessary for discovering such evidence.' Pursuant to Chapter 9 Article 355P of the Criminal Code – *'The Police, when lawfully on any premises, may seize anything which is on the premises if they have reasonable grounds for believing that it has been obtained in consequence of the commission of an offence or that it is evidence in relation to an offence or it is the subject of an alert in the Schengen Information System and that it is necessary to seize it to prevent it being concealed, lost, damaged, altered or destroyed.'* Pursuant to Chapter 9 Article 355Q of the Criminal Code, *'The Police may, in addition to the power of seizing a computer machine, require any information which is contained in a computer to be delivered in a form in which it can be taken away and in which it is visible and legible.'* With reference to point Article 19.3 d - *'render inaccessible or remove those computer data in the accessed computer system.'*, the magistrate may communicate to the competent authority to proceed with the removal of the content or part thereof. This communication can be made available via a warrant/decree.	
Mauritius	Seizures as described in Article 19.3 are governed by Section 28 and follow the same procedures as for searches as in Article 19.1. A court has the power to authorise a seizure. The police (and the Financial Crimes Commission) execute the seizure. Section 28 essentially duplicates the language of Article 19.3. Thus Mauritius clearly has the power to carry out all four elements of Article 19.3. Applications for searches, and the orders that proceed from such applications, specify the parameters of the intended search. If extension of a search is needed, a second order must be procured. It is unlikely that a court would permit extension of a search when the location of the data is unknown.	Mauritius applies specific search and seizure powers to implement Article 19.3.
Monaco	Authorities pointed out that domestic law provides for specific mechanisms for seizing or securing computer data as part of an investigation or judicial inquiry (Art. 255 of the CPC).	Monaco applies a combination of general and specific search and seizure powers to implement Article 19.3.

Party	Legislative and other measures	Assessment
	Art. 255 provides a legal basis for copying and deleting computer data whose possession or use is illegal or dangerous to the safety of persons or property. Originals of software are secured and exact copies are made. Alternatively, software is sent to an expert when the investigators cannot handle it on their own.	
Montenegro	Provisions of provisional seizure of the CPC apply. Art. 85.4 extends the application to the data saved in devices for automatic or electronic data processing and media wherein such data are saved. The data saved in devices for automatic or electronic data processing and media wherein such data are saved shall be handed over upon the request of the court, in a legible and comprehensible form. The court and other authorities shall abide by the regulations on maintaining data secrecy. It is however, not clear how is Art. 19.3 d) of the Convention implemented in the domestic law. The authorities have not indicated how they proceed in cases when extending a search and in situations when it cannot be determined where the data sought are stored. However, the search warrant shall specify all the details regarding the objects of search and seizure. At the same time, a new search and seizure warrant may be requested in the case of need for search of another computer system.	Montenegro applies a combination of general and specific search and seizure powers to implement Article 19.3. Further clarification on implementation of Art. 19.3 d) would be desirable.
Morocco	It should be noted that Morocco is in the process of updating its legislation. In the meantime, its criminal procedure mechanisms are close in practice to the requirements of the Convention. Thus, elements a through d of Article 19.3 may be satisfied by Moroccan procedure. There are indications that Morocco can meet at least some of those elements via current statutes – for example, Article 104 of the CPC mentions the inventorying and protection of articles that have been seized. There is no apparent power to remove data or render them inaccessible. The usual procedures for authorising and conducting a search apply, without discriminating specifically which may correspond to electronic evidence and stored electronic data. Technical expertise is available.	Morocco applies general search and seizure powers to implement Article 19.3. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty. More clarification regarding implementation of specific elements a through d of Art. 19.3. could be beneficial.
Netherlands	Criminal Procedure Code doesn't contain specific provisions on seizing computer-related data, but the general seizure provisions can be used to seize data storage devices. Art. 125i of the Criminal Procedure Code introduces the power to search and to preserve data. Data as such cannot be seized, since they are not considered "goods", but they may be copied by law enforcement officers during a search.	Netherlands applies a combination of general and specific search and seizure powers to implement Article 19.3.

Party	Legislative and other measures	Assessment
	The authorities reported that they have the following legislation: When a suspect is arrested or detained the following articles apply: Art. 53-55b DCCP and 95-96 DCCP 19 para 3 CCC. When a place (other than a home) is searched the following articles apply: Art. 96 DCCP, Art. 96b DCCP, Art. 96c DCCP and Art. 110 DCCP 19 paragraph 3 CCC. In the interest of public order or the protection of victims, Article 125p of the Criminal Procedure Code, allows the prosecutor to order an internet service provider to make the content inaccessible and in some cases, with judicial order, the definitive deletion of the data (Art. 354 Criminal Procedure Code). The hacking power of Art. 126nba, lid 1, sub e, DCCP, also allows for making data inaccessible, if the data is found in an automated work regarding which or with the aid of which a criminal offense was committed. In that case, the public prosecutor may determine that these data are made inaccessible insofar as this is necessary to end the criminal offense or to the prevention of new criminal offences. The measures described are also applicable on the extension of search situations.	
Nigeria	The procedures and requirements in Section 45 of the Cybercrimes Act, previously described, govern seizures as in Budapest Article 19.3. The authorising and executing authorities are the same. The same measures are applied when extending a search per Article 19.2 and in situations when the location of the data cannot be determined.	Nigeria applies a combination of general and specific search and seizure powers to implement Article 19.3. However, it is not clear how the powers to make and retain a copy of data, maintain the integrity of data, and remove data or render it inaccessible per Article 19.3 b-d are implemented in Nigeria. Provisions specific to computer data and systems could permit greater clarity and legal certainty.
North Macedonia	The requirements, procedural steps, and authorities involved in seizures under Article 19.3 are the same as described above as to Article 19.1. They are also the same as for extensions of searches under Article 19.2 and when the location of data is unknown.	North Macedonia applies a combination of general and specific search and seizure powers to implement Article 19.3. Provisions specific to computer

Party	Legislative and other measures	Assessment
	Articles 194 and 198 of the CPC refer to the safekeeping of seized items, including computer data. CPC Articles 184, 194 and 198 provide for copying of electronic evidence. In conjunction with standards of the MOI's forensic laboratory, those CPC articles provide for protecting the integrity of the data. However, the CPC articles do not relate to one of the other elements of Budapest 19.3: removing data or rendering them inaccessible.	data and systems could permit greater clarity and enhance legal certainty, particularly regarding removing data or rendering them inaccessible, which does not seem to be possible.
Norway	Two sections of the CPC and Section 7 of the Police Act combine to satisfy the elements of Article 19.3 a through d. In particular, Article 203 authorises the removal of physical objects and, implicitly, the rendering inaccessible or removal of computer data. Beyond this, the statutory power of the police to prevent or stop offences may be used to order that data be rendered inaccessible, for example to prevent the spread of malware. Norway supplied further detail and examples regarding this power. In general, the same provisions apply in cases where the data's location is unknown as in extensions of searches. Good faith, proportionality and international cooperation are taken into consideration. The authorities involved are the same.	Norway applies general search and seizure powers to implement Article 19.3. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.
Panama	The legal basis for seizure is Article 308 of the Criminal Procedure Code. The regulation does not specifically refer to computer systems or storage devices, but it is sufficiently broad to achieve this purpose. There is no specific regulation to implement what is established in Article 19.3d. It should be noted that the authorities mentioned the procedural regulations allow for the seizure of any type of instruments used in the commission of a criminal act. The regulation does not specifically refer to computer systems or storage devices, but it is sufficiently broad to achieve this purpose. Panama applies the same measures when extending a search (according to Article 19.2) and in situations when it cannot be determined where the data sought are stored. The authorities that authorise a seizure are the Judge as the judicial authority. The authorities that carry out a confiscation are the Public Prosecutor's Office, acting through the different prosecutors' offices, as the competent authority. About technical experiences, Article 298 of the Code of Criminal Procedure establishes the exceptions in which a search and seizure may be carried out without judicial authorisation, if it is necessary to prevent the commission of a crime or in case of flagrante delicto. This article also applies when the Prosecutor who carries out the search determines	Panama applies a combination of general and specific search and seizure powers to implement Article 19.3. It seems that Art. 19.3d needs to be implemented into domestic law. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.

Party	Legislative and other measures	Assessment
	that there is a danger of loss of evidence or if it is derived from an immediately previous search. In these cases, this exceptional search procedure must be submitted to the control of a Judge of Guarantees (as a subsequent control).	
Paraguay	The Paraguayan Criminal Procedure Code includes provisions for the seizure and safeguarding of evidence, including digital evidence. According to Article 196 of the code, the procedure for registration will be followed. The seized effects or items will be inventoried and securely stored in designated locations under the custody of the courts. In the case of valuable items, they may be delivered to legitimate possessors acting as judicial depositories. In cases where the seized objects are at risk of alteration, disappearance, or difficulty in preservation, reproductions, copies, or certifications of their existence and condition may be ordered. According to the information provided by the Paraguayan authorities, compliance with the provisions of Article 19.3 is based on analogical interpretations allowed by the principle of freedom of evidence. After any search or seizure, it is the obligation of the Public Prosecutor's Office to report what was found and not, whether for traditional or digital evidence. The competent authorities that authorise a seizure: by order of a competent criminal judge, at the request of the Public Ministry, and then referral to the National Secretariat of Seized Assets.	Paraguay applies general search and seizure powers to implement Article 19.3. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.
Peru	With respect to the application of the seizure of stored computer data, it is provided for in articles 214°, 217°, 316° and 318° of the Criminal Procedure Code, a measure that is executed in merit of a judicial resolution or of entailing an extension of the search through a judicial validation of the confirmation of the seizure of goods. Provisions of Chapter V, Chapter VI, Chapter VII, Chapter VIII and Title X of the Criminal Procedure Code, Law 27697 – Law that grants power to the Prosecutor for the Intervention and Control of Communications and Private Documents in exceptional cases apply by analogy. In this relation, the Peruvian authorities have interpreted that Article 19, paragraph 3, subparagraph a) of the Budapest Convention, can be achieved by means of "seizure" in accordance with the Criminal Procedure Code , as well as with regard to paragraphs b) and c), is liable to be applied by means of the measure of "inspection" as provided for in the Criminal Procedure Code , among others that will be applied according to each specific case.	Peru applies general search and seizure powers to implement Article 19.3. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.

Party	Legislative and other measures	Assessment
	Peruvian Authorities refer that the same measures are applied in an extension of the search through the validation of the requirement on the confirmation of the seizure of assets, in accordance with what is indicated in the procedure established in Title X of the Criminal Procedure Code. Regarding the situations in which it is not possible to determine where the searched data are stored, failure to comply with this obligation may result in criminal, civil, or administrative consequences, depending on the circumstances. If possible, seizure of the servers can be done. The authorities in compliance with the Law, such as Prosecutors of the Public Prosecutor's Office for example, may request the Judge the authorisation and execution of the measure limiting the right of "seizure" on those data that are recorded, which may be subject to validation if during the execution of the measure any extension of the search was made, without detriment to the validity of the execution of the "seizure" measure even if the data were stored in another computer system, as provided for in articles 214°, 217°, 316° and 318° of the Criminal Procedure Code. The execution of restrictive seizure measures is required by the Prosecutor, authorised by the Judge through a duly reasoned resolution, and executed by the Prosecutor and/or the National Police, the personnel who execute the measure must have minimally basic computer knowledge to carry out a successful procedure. Restricting measures are applied to stored computer data and data storage media in the territory, considering the provisions of Chapter V, Chapter VI, Chapter VII, Chapter VIII and Title X of the Criminal Procedure Code, Law 27697 -which grants power to the Prosecutor for the Intervention and Control of Communications and Private Documents in exceptional cases, and the correct Criminal Procedure Code. This law plays a supplementary role in cases involving the lifting of the secrecy of communications, and unlike Article 230° of the Criminal Procedure Code, it lists various crimes, including those related to computer crimes outlined in Law N°30096. The Prosecutor can use this law to support rights-limiting measures when necessary to lift communication secrecy and access stored computer data. However, it emphasizes that this does not modify the legal basis established in Article 230° of the Criminal Procedure Code, which imposes different formal requirements rather than listing specific crimes.	
Philippines	The procedures and requirements for searches under Article 19.3 are the same as previously described, and the same authorities and experts are involved. The same measures are applied when the location of data is unknown as when a search is extended under Article 19.2. The Cybercrime Prevention Act expressly provides for making and retaining copies of data, maintaining their integrity, and removing data or rendering it inaccessible:	The Philippines applies specific search and seizure powers to implement Article 19.3.

Party	Legislative and other measures	Assessment
	SEC. 15. Search, Seizure and Examination of Computer Data. — Where a search and seizure warrant is properly issued, the law enforcement authorities shall likewise have the following powers and duties. Within the time period specified in the warrant, to conduct interception, as defined in this Act, and: (a) To secure a computer system or a computer data storage medium; (b) To make and retain a copy of those computer data secured; (c) To maintain the integrity of the relevant stored computer data; (d) To conduct forensic analysis or examination of the computer data storage medium; and (e) To render inaccessible or remove those computer data in the accessed computer or computer and communications network.	
Poland	Poland's thoughtful and detailed response cited numerous CPC articles and police regulations to satisfy the elements of Article 19.3. The applicable legislation does not provide for a separate procedural step to preserve digital evidence. Therefore, the indicated provisions also refer to parts b and d of Article 19. In cases in which it is not necessary to secure the data together with the medium, a full duplicate of the content of a given medium in the form of its binary copy is made. Pursuant to CPC Article 218 a § 4, the court or the public prosecutor may order the deletion of content if its publication or communication constitutes a prohibited act. However, it appears that the power of deletion may be used only in relation to offices, institutions, and entities carrying out telecommunications activities or supplying electronic services and providers of digital services and seems to be applicable to data that were already published or to which the access was granted. This does however not encompass all the scenarios where data are stored in the computer system of the suspect (non-public data) and are accessed by competent authorities. It seems that the power of copying is regularly exercised in practice, however, the exact legal basis of this measure remains not clear enough.	Poland applies a combination of general and specific search and seizure powers to implement Article 19.3. More specific provisions to implement Art. 19.3.b. and d could permit greater clarity and enhance legal certainty.

Party	Legislative and other measures	Assessment
	The same measures are used when the location of data is unknown as when extending a search. The authorising and executing authorities are the same.	
Portugal	Article 16 of the Cybercrime Law writes into Portuguese law all the powers in Article 19.3 of Budapest. The same measures are applied in cases of extension of searches and searches in whose case the location of the data is unknown. Doctrine and jurisprudence about integrating the possibility of extension of searches into legal and judicial practice are not fully settled. However, access to a remote computer system is only permitted in the course of a search. When such a search is conducted, the procedure is the same as for a "local" search. One of the forms of seizure provided for in article 16 of the Cybercrime Law will be used. They are equivalent to those described in article 19, paragraph 3, of the Budapest Convention. In practice, investigators access the remote system and, if necessary, for example, make a copy of relevant data. The authorities involved in the process are as described above.	Portugal applies specific search and seizure powers to implement Article 19.3.
Republic of Moldova	The procedures for seizing or securing data per Article 19.3, and the authorities involved, are the same as in searches pursuant to Article 19.1. The procedures for extending a search per Article 19.2 *and* when the location of the data cannot be determined (and the authorities involved) are the same as in searches pursuant to Article 19.1. Moldova does not have legislative provisions for removing data or rendering them inaccessible. However, Article 128 of the CPC, a general provision, permits law enforcement/prosecutors to examine data and to remove them from all seized devices.	Moldova applies a combination of general and specific search and seizure powers to implement Article 19.3. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.
Romania	Article 168 of the CPC and standard search and seizure procedures provide for elements a through c of Article 19.3. As regards Article 19.3d, the computer or internal or standalone storage devices are considered corpus delicti according to the law. They are therefore subject to a seizing order during the criminal investigation and are subject to confiscation at the conclusion of trial. Corpus delicti may be confiscated even if a prosecutor drops a case as a minor offence.	Romania applies a combination of general and specific search and seizure powers to implement Article 19.1. It appears that Art. 19.3.d. has not been implemented. Provisions specific to

Party	Legislative and other measures	Assessment
	However, there is no indication in the text with respect to the seizing of computer data, rendering inaccessible or removing computer data in the searched computer or device. The usual authorities are involved in searches relating to Article 19.3.	computer data and systems could permit greater clarity and enhance legal certainty.
San Marino	Search and seizure of computer data is conducted according to the same procedures as for physical evidence. Although the applicable law does not sufficiently cover elements b-d of Art. 19.3. of the BC, authorities stated that general powers of the domestic legal system may encompass these powers. Several articles of the CPC provide for integrity of evidence. Authorities stated that the removal and inaccessibility of data is subject to an explicit order issued by the competent Judicial Authority. Law no. 24 of 2 March 2022, "Provisions to implement the guarantees and the efficiency of criminal proceedings" and operational procedures for executing seizures in general complement the legal framework. Article 58-quinquies allows for the preventive seizure of assets when there are reasonable grounds to believe that they may be used to aggravate or extend the crime in question, or to facilitate further criminal activity. It is the responsibility of the judge to issue a detailed decree which limits the scope of the seizure. To ensure the extraction of relevant data, key words are often used. The forensic copy of the data is an independent entity, and any superfluous data must be returned to the rightful owner. The legislation includes safeguards to prevent undue invasions of privacy. If these protections are violated, the seizure may be annulled. It seems that San Marino does not have any established procedures for addressing instances where the location of stored data is undeterminable. The Court grants delegated powers to carry out investigations, searches and seizures; the police forces execute such delegated powers or act on their own initiative in case of specific crimes. In order to analyze the data, files and hardware that have been seized, the officers of the police forces, again upon mandate of the Judiciary, collaborate with specialized technical experts or assign specific tasks to them.	San Marino applies general powers to implement Article 19.3. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.

Party	Legislative and other measures	Assessment
Senegal	Articles 90-1 to 90-14 of the CPC provide for the authorities to seize or similarly secure electronic data or information systems, to copy and maintain the seized data, to preserve their integrity, and to remove them or render them inaccessible. The same measures are applied when searches are extended and in situations when the location of the data cannot be determined. The authorities that authorise and carry out seizures are the same as described above.	Senegal applies specific search and seizure powers to implement Article 19.3.
Serbia	The numerous articles of the CPC discussed above and the standard operating procedures of the law enforcement agency involved provide for the implementation of Article 19.3. Several articles provide that "movable things" can include computer data, devices, carriers and programs that may be temporarily seized to be held as evidence or examined by forensic experts. The law enforcement agency and digital forensic standard operating procedures provide for copying of data from the original repository. Electronic data that are accessible via computer networks or other remote means can be removed or rendered inaccessible 1) by the seizure itself, per the CPC and standard operating procedures for securing a crime scene, or 2) on the grounds of securing the evidence and preventing its destruction, removal or alteration, similar to SOPs for securing a crime scene. The same measures are applied when extending a search and in situations when the location of data cannot be determined. Public prosecutors request a seizure, courts allow or order it and the police execute it. Specialised units within the police have the necessary expertise.	Serbia applies a combination of general and specific search and seizure powers to implement Article 19.3. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty, in particular regarding Art. 19.3.b.
Sierra Leone	To enable seizure or secure access to computer data, the enforcement officer shall make an application for a warrant to a High Court Judge under section 10 (1). This warrant can be used as an authorisation to access, seize, or secure a computer system, program, data or computer data storage medium that may be required as evidence in proving an offense in a criminal investigation or criminal proceedings or has been acquired by a person because of the commission of an offense. A warrant issued shall authorize an enforcement officer to seize or secure a computer system or part of it or a computer data storage medium and covers also elements of letters b-d of Art. 19 of the BC.	Sierra Leone applies specific search and seizure powers to implement Article 19.3.

Party	Legislative and other measures	Assessment
	Sierra Leone reported that they apply the same measures when extending a search and in situations when it cannot be determined where the data sought is stored. The competent authorities that authorize the measure are judges and carry out a seizure as described in Article 19.3 are law enforcement officers like the police and other competent authorities.	
Slovak Republic	Seizure of the computer hardware and storage media is possible under the general powers for Section 89a obligation "to issue the thing." Based on a previous request, the person must be informed of the consequences of non-compliance and the fact that this thing, which can be used for the purposes of evidence, can be taken away and Section 90 confiscation of a thing – occurs in the event of non-issue of a thing that can be used for the purposes of evidence. To obtain computer data from things secured in this way, or computer data storage media, no further command is needed. The Supreme Court of the Slovak Republic has already decided on this, as part of its decision-making activity. Section 91.1 b) of the CPC appears to meet requirements of Art. 19.3 b) of the Convention. The authorities may order any person to remove the data from the computer system. The integrity of the computer data is guaranteed via the hash (MD5 but SHA-1) values of the secured computer data. This is done by a forensic technician or expert when securing a trace or computer data. Authorities informed that the same procedures are used in extensions of search and when the location of data is unknown – that is, an attempt is made to determine the location of the data.	Slovak Republic applies specific search and seizure powers to implement Article 19.3.
Slovenia	Articles 219a and 223a of the CPC seem to cover subparas a through c of Article 19.3. Slovenia has the power to remove data or render them inaccessible pursuant to Article 498 of the CPC. Article 498 is a detailed general provision for confiscation of objects. In the case of electronic data, the seized objects are data carriers. However, it seems that the provision does not apply to computer data and thus it may be problematic to apply such a rule when there is a need to "render inaccessible or remove computer data", but not the storage medium where the data are stored.	Slovenia applies a combination of general and specific search and seizure powers to implement Article 19.3. It appears that Slovenia implemented Art. 19.3.d. solely through general search and seizure powers. Provisions specific to computer data and systems

Party	Legislative and other measures	Assessment
	It appears that the same measures are used, and the same authorities are involved, in cases of extended search as in cases where the location of the data cannot be determined. The emphasis is on authorisation by an initial warrant or a subsequent warrant, assuming that subsequent systems or devices are accessible from the initial item. However, the procedures are unclear in cases when the data's location is unknown.	could permit greater clarity and enhance legal certainty.
Spain	Article 588sexies (c) of Criminal Procedure Code (LECrim) allows for the seizure and copying of physical media that may contain relevant data, provided that appropriate conditions are met to ensure the authenticity and integrity of the data. The judge in charge of the investigation is responsible for authorising the search and seizure of data and deciding on the most appropriate course of action. The Spanish legislator entrusts the judicial authority with establishing the necessary conditions to guarantee the integrity and preservation of the data for expert opinions, which will be evaluated on a case-by-case basis depending on the circumstances of the investigation. In sum, Spanish procedural law provides that the judge is in charge of deciding the specific manner in which the seizure of data will be carried out. The only measures referred to in article 19.3 of the Convention expressly referred to in the Spanish legal text are the making and retention of copies of data and the confiscation or seizure of the computer device. In practice, the judge may also order the seized information to be stored in the computer system subject to registration, although the access passwords are changed, with judicial authorisation, so that the information is preserved and cannot be accessed by the investigated itself or by third parties outside the investigation. The same standards are upheld in cases where evidence is located on cloud storage or foreign servers, but the context is considered. If access to the evidence is available from the equipment that was initially registered, but the location of the evidence is unknown, appropriate procedural guarantees, in accordance with Spanish legislation, and judicial authorisation are required to access it.	Spain applies specific search and seizure powers to implement Article 19.3.
Sri Lanka	Sections 18 and 20-22 of the Computer Crime Act are used to implement Article 19.3 seizures. Per Section 22 of the CCA, Sri Lanka has the power to remove data or render it inaccessible ("where any item or data has been seized or rendered inaccessible in the course of an investigation, the police officer conducting the search shall issue a complete list of such items and data including the date and time of such seizure or of rendering it inaccessible to the owner or	Sri Lanka applies a combination of general and specific search and seizure powers to implement Article 19.3. Provisions specific to computer data

Party	Legislative and other measures	Assessment
	person in charge of the computer or computer system"). Some elements of the powers to copy data for the use of criminal justice officials and maintain its integrity may be implied in the CCA (The CCA permits copies to be made for a third party under certain circumstances). The same measures are applied when searches are extended per Article 19.2 and in situations when the location of the data cannot be determined. The police are the authorities that execute seizures. They may be assisted by Sri Lanka CERT and court-appointed experts.	and systems could permit greater clarity and enhance legal certainty.
Sweden	The CPC through its general rules provides for seizures of objects. The general rules provide for maintenance of the integrity of data as well as removing data or rendering them inaccessible. Copying of electronic data is provided for by Section 17a, Chapter 27, of the Code. When the location of data cannot be determined, the same copying measures may be utilised as with extended searches. Authorisations and conduct of the procedures are the same.	Sweden applies a combination of general and specific search and seizure powers to implement Article 19.3. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty, particularly regarding Art. 19.3.d.
Switzerland	The authorities have the power to search, seize and copy data. The responses indirectly indicated that there are procedures to satisfy Article 19.3 c – that is, to protect the integrity of the evidence, including by isolation from networks. As for Article 19.3d, removing data or rendering them inaccessible, Article. 69 of the Criminal Code provides that the court shall, irrespective of the criminal liability of any person, order the forfeiture of objects used or intended for use in the commission of an offence or that have been produced as a result of the commission of an offence if those objects constitute a future danger to public safety, morals or public order. The prosecutor can also issue such order when he issues a criminal order (ordonnance pénale). The same procedures are employed, and the same justice system officials are involved, when searches are extended as when the location of the data is unknown.	Switzerland applies a combination of general and specific search and seizure powers to implement Article 19.3.

Party	Legislative and other measures	Assessment
Tonga	Pursuant to Section 9 of the Computer Crimes Act, the police may search and seize computers and data and copy and maintain data. The Computer Crimes Act in its Art. 2 specifies that term "seize" includes also removal or rendering the data inaccessible. The same measures are applied when searches are extended and when the location of the data cannot be determined; there is no specific legislation on this topic. Whether a search may be extended to seize or similarly access computer systems or data depends on what the search warrant specifically states – that is, whether it includes any computer systems that may be connected or linked to the device of interest. Such extensions have been practiced and successfully used in police investigations. In the past, when location data was lost or deleted and could not be determined, IT experts from the Australian Federal Police and New Zealand Police and local contractors have carried out a data recovery process in sensitive and significant investigations only. In addition, when the location of data cannot be determined, support and technical assistance will be sought from foreign experts through collaboration with CERT. Magistrates authorise seizures pursuant to Article 19.3. Seizures are executed by police officers, possibly in conjunction with CERT Tonga, and occasionally with the assistance of foreign forensic experts.	Tonga applies a combination of general and specific search and seizure powers to implement Article 19.3.
Tunisia		
Türkiye	Article 134 of the CPC and Article 17 of the Bylaws on Judicial and Preventive Searches seem to provide for elements a through c of Article 19.3. Türkiye supplied extensive detail about its law and search practices, emphasizing the protection of digital evidence. For example, it mentioned focusing on the particularities of computer systems, ensuring that only qualified specialists (rather than less-trained officers) work on the electronic data, and using video records, forensic packaging, HASHing, write-protection and so on. It is not clear whether Türkiye has the power to remove data or render them inaccessible. The procedures for searches and seizures, and the officials involved, are the same when searches are extended and when the location of the data is unknown.	Türkiye applies specific search and seizure powers to implement Article 19.3. Further clarification regarding implementation of Art. 19.3.d. would be desirable.
Ukraine	Article 159 of the Criminal Procedural Code of Ukraine provides for temporary access to electronic information systems, computer systems or parts thereof, mobile terminals of communication systems, which is carried out by taking a copy	It appears that Ukraine applies a combination of general and specific

Party	Legislative and other measures	Assessment
	of the information contained in such electronic information systems, computer systems or parts thereof, mobile terminals of communication systems, without their withdrawal. Issues related to maintaining the integrity of relevant stored computer data; to make inaccessible or delete this computer data in the computer system to which access is carried out appears to not be regulated in the legislation of Ukraine. It seems that implementation of specific elements as described in Article 19.3. requires additional legislative regulation by introducing appropriate amendments to the Criminal Procedure Code of Ukraine.	search and seizure powers to implement Article 19.3. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty,
United Kingdom	The UK authorities informed that the powers in PACE permit to seize or similarly secure computer data while the activity itself will be carried out using operational processes set out in police training procedures. The general power of seizure is extended through legislation to cover computerized information. This is the case of England, Wales and Northern Ireland. In Scotland, there are no separate and distinct legislative measures to seize or secure computer data. Where there is a power of search, it is taken that there will be a power to seize what is found during the search. In practice, electronic devices are often copied or 'imaged' instead of seized. The power to copy electronic data from devices is explicit under the Criminal Justice and Police Act 2001. There are no provisions specifically governing the treatment of computer data seized pursuant to a search warrant. Instead, the way in which such material is handled is regulated by the provisions which govern the treatment of material generally. Furthermore, under PACE, there is a general power for constables to retain seized or produced material for so long as is necessary. Where seizure is for the purposes of a criminal investigation, material may be retained for use as evidence at a trial for an offence, for forensic examination or for investigation in connection with an offence. Where electronic information is accessible from premises, a constable can require production of this material "in a form in which it can be taken away and in which it is visible and legible or from which it can readily be produced in a visible and legible form. General powers of seizure that are extended to cover computer data (Section 19, 20 and 22 of the PACE 1984) allow law enforcement to physically remove storage media and thus render data inaccessible where a constable is lawfully on the premises.	United Kingdom applies a combination of general and specific search and seizure powers to implement Article 19.3. The scope of the measure to render inaccessible or remove computer data from a computer system that is being accessed, as established in domestic law, appears to be limited to situations where the authorities are on the premises and does not extend, for example, to situations where a computer system is searched on the premises of the law enforcement authorities. Provisions specific to computer data and systems creating a legal framework for the search and seizure of computer data and systems applicable in England, Scotland, Wales

Party	Legislative and other measures	Assessment
	The competent authorities are the same as in relation to search. The technical expertise required will depend on the case, but appropriately trained officers from cybercrime units at national, regional, or local level may be involved to ensure that the material is managed correctly.	and Northern Ireland could permit greater clarity and enhance legal certainty.
United States	The same measures and procedures are used in extension of searches and when the location of the data is unknown. The same justice system officials are involved. The procedures described include the ability to search, seize and copy data. The US has the power to maintain the integrity of seized data. This obligation derives from a defendant's constitutional rights to a fair trial and due process and (among other sources) the Federal Rules of Evidence, which require that data be identified and authenticated in order to be used at trial. Law enforcement agencies have policies regarding the "chain of custody" of all criminal evidence. Data may be rendered inaccessible via the execution of a search warrant, since it is usually seized and maintained in the possession of law enforcement.	The United States applies a combination of general and specific search and seizure powers to implement Article 19.3.

7 ORDERING A PERSON TO ENABLE THE SEARCH AND SEIZURE OF STORED COMPUTER DATA (ASSESSMENT OF ARTICLE 19.4)

This section assesses implementation of Article 19.4:

> Article 19 – Search and seizure of stored computer data
>
> 4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.

7.1 Implementation of Article 19.4: overview

7.1.1 Legislative and other measures - summary

Article 19.4 requires Parties to have the power to order "any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein" to provide, as is reasonable, the information necessary to fulfil the aims of the search. It should be noted that this is without prejudice to domestic law safeguards, such as the right against self-incrimination (see also next Chapter). It appears that the compliance of many Parties with this requirement may be unclear. As implemented by many Parties, this power focuses on owners or users of systems, often system administrators, IT staff or business employees. This focus may be sufficient most of the time, but it is not broad enough to capture less-expected categories of people who may have useful knowledge. Parties are encouraged to ensure that they have the same authority to compel assistance from third parties in searches of computer systems that they have to compel assistance from third parties in searches of physical locations.

As a practical matter, authorities executing searches may be able to deal with such situations. But it seems that there is a tendency, especially in statutory text, to limit the "any person" of Article 19.4 to owners or users of data. In addition to this, there are a number of Parties that implement this provision via production orders which empower the competent authorities to order a person in their territory to submit specified computer data in that person's possession or control. Although in certain cases the provision of the "necessary information" could cover the disclosure of the actual data that are being sought, Article 19.4 requires the disclosure only of "necessary information" which is "reasonable". In some circumstances, where consistent with domestic legal frameworks, reasonableness may include disclosing a password or other security measure to the investigating authorities and not disclosing the data per se. Therefore, Parties that implemented the obligation under Article 19.4 of the Convention on Cybercrime through production orders, must demonstrate that "necessary information" may include different types of information and not solely the data per se.

Some Parties also indicated that system administrators or other persons who have particular knowledge of the computer system may provide their assistance voluntarily but cannot be obliged to do so. However, this does not sufficiently meet the requirements of Article 19.4, as the provision requires the establishment of an obligation on persons to provide the necessary information. Legally compelling a system administrator to assist may also relieve the administrator of any contractual or other obligations not to disclose the data. It should be noted that this is without prejudice to domestic law safeguards, such as the right against self-incrimination (see also next Chapter).

A number of Parties require a prosecution or court order before someone's assistance can be compelled. In some cases, it appeared that the authorities could apply for an order requiring

assistance when they apply for a search warrant. (The need for a warrant or authorisation to compel a person to cooperate may be important in terms of safeguards, especially in those Parties where failure to comply may result in a criminal charge.)

A warrant application may not require the authorities to specify whom they will need to compel at the time of application.

But if the authorities do not have such knowledge, or if there are surprises once the search begins, then the search may need to be delayed or halted for a subsequent application for an assistance order.

In such cases, a Party would still be in line with Article 19.4, because it could in fact compel assistance.

Examples of elements that can be found in the domestic laws or practice of the Parties:[60]

- Andorra: Article 397 (disobedience) and Article 427.1 (hindrance) of the CC provide for criminal penalties (as a minor offence) for anyone who does not follow the order of competent authorities.

- Australia: Section 3LA of Crimes Act provides for an order requiring a specified person to provide any information or assistance that is reasonable and necessary to allow a constable to access data held in a computer or data storage device.

- Austria: Article 111.2 of the CCP regulates that, if information saved on data storage mediums has to be secured, any person has to grant access to that information.

- Belgium: Article 88.1 quater obliges any persons with particular knowledge of the practical and specific aspects of computer technology to provide information on access possibilities, configuration, protection and encryption keys. Article 88.2 extends this obligation to persons to carry out certain actions, when necessary (starting up the computer, searching for files, etc.).

- Brazil: Courts may order temporary suspension of internet service providers' activities and the payment of fines, in order to comply with court orders to provide requested information. Moreover, according to Art. 378 Code of Civil Procedure, no one is exempt from the duty to collaborate with the judiciary in discovering the truth.

- Bulgaria: Generally, each and every person is obliged by law to cooperate with the investigation authorities and to share everything he/she knows when questioned.

- Canada: Section 487(2.2) explicitly provides that a person in charge of a building or location may be required to permit access to and retrieval of data.

- Costa Rica: Under Article 7 of the Organic Law of the Judicial Power, a judge can order any person to help with the investigation according to their field of knowledge.

- Croatia: Under Article 257.2 CCP, any person using the computer or having access to the computer and other devices or the telecommunications service provider shall immediately undertake measures for preventing the destruction or change of data.

[60] These examples may or may not meet the requirements of Article 19.4. They show the range of responses.

- Cyprus: Authorities may ask for system administrators' cooperation; cooperation cannot be compelled.

- Czech Republic: According to Article 8 of the CPC it is possible to request cooperation from physical and legal persons and to impose a fine in case of not obeying such request.

- Denmark: Under Section 747of the AJA, court approval may be sought for measures that require assistance or to secure evidence which may be lost or be available only with significant inconvenience or delay.

- Dominican Republic: Article 54 of law 53-07 provides for power to order any person who knows about the operation of an information system or any of its components or of the data protection components or the data protection measures in such a system to provide the necessary information.

- Estonia: In case a person can be considered as a witness, then he/she has obligations to provide information. Under Article 95 of the CPC, an expert is "a person who applies non-legal specialised knowledge when conducting an expert assessment in situations and following the rules provided by this Code."

- Finland: Coercive Measures Act stipulates the obligation of a person who owns or maintains an information system or any other person to provide necessary information (such as password) and assist the authorities when needed.

- France: 2 offences specifically target the refusal to assist authorities - Refusal to hand over to the authorities or to implement the secret decryption agreement for a cryptology device (Article 434-15-2 dal1 of the CC) and Refusal to hand over to the judicial authorities or to implement a secret decryption agreement for a cryptology device when this refusal has not enabled the commission of an offence to be avoided (Article 434-15-2 para 2 of the CC).

- Georgia: According to Article 112 of the CPC, investigators and/or other law enforcement officers executing a search warrant must first ask the persons responsible for the search site (e.g. system administrators) to voluntarily provide relevant information. If there is no compliance, investigation can resort to compelled enforcement.

- Germany: According to Section 95 (1) of the CPC, persons who are not suspected of any crime could be obliged to hand over access codes or talk about their knowledge about the functioning of a computer system.

- Hungary: Sections 267 and 271 of the CPC establish the power in general for the authorities to collect criminal evidence and to request relevant information from any person while Section 305 provides that authorities may require a person to make electronic data accessible.

- Iceland: Article 92 of the Act no. 70/2022 on Electronic Communications obliges telecommunication companies to assist the police in criminal investigations.

- Israel: Article 45 of the Criminal Procedure Ordinance requires the occupant of the place for which a search warrant has been granted to provide entry and any reasonable assistance.

- Japan: Authorities may require persons to assist the search or seizure, in particular to operate the computer, and to cooperate in other ways (Article 111-2 and 222 of the CPC). "To operate the computer, or for some other form of cooperation" under Article 111-2 of the Code of Criminal Procedure may include, for example, (1) explaining the composition of a computer system and the roles, functions, and operation methods of the individual computers composing the computer system, (2) giving instructions on the location of recording media to be seized, and (3) decrypting encrypted electronic or magnetic records.

- Latvia: According to Article 190 of the CPC, the authorities may obtain electronic information from persons affected by searches and seizures. Such mechanism does not provide for sanctions, persons may cooperate voluntarily.

- Liechtenstein: Several sections of the CPC provide for requiring persons to assist in a seizure and to compel such assistance if it is refused.

- Lithuania: Article 97 of the CPC states that natural and legal persons must produce objects and documents relevant to the investigation. Article 219a of the CPC provides that the owner or user of an electronic device must provide access to it, including decryption and explanations about its use, and facilitate the investigation.

- Montenegro: Article 75.2 of the CPC obliges users to provide necessary information, Article 83.3 and 83.4 obliges persons to hand over relevant items.

- Morocco: The law obliges licensed public telecommunications networks and service providers to assist the judicial authorities.

- Netherlands: Article 125k of the CPC empowers competent authorities to compel a person who can reasonably be presumed to have knowledge of the security arrangements of a computerised work to provide access to and knowledge about the computerised works or parts thereof and its security measures. A similar order may be addressed to the person who can reasonably be suspected of having knowledge of the encryption method used for data. Certain limitations exist with respect to specific categories of persons (for example, persons who might self-incriminate).[61] Under Article 558 DCCP, people can be forced to submit to certain "forced actions" for biometric access to a device that is locked by fingerprint or face ID (if the action can be done without obliging people to wilfully do something themselves). Laying a thumb on the smartphone or bringing the smartphone in front of a person's face can be done without forcing the person to give the credential.

- Norway: When searching a computer system, the police may order anyone who has dealings with the computer system to provide the necessary information to allow access to the computer system or to open it using biometric authentication. If order for biometric authentication is refused, police may carry out the authentication by force.

- Panama: Article 75 of the CPC establishes obligation to cooperate, applicable to both public and private entities, in a prompt, effective and complete manner to the requirements formulated by the competent authorities.

- Peru: According to the Article 337.3 b) of the CCP, competent authorities can request information from any person. Failure to comply with these formulated requirements may result in the criminalization of resistance or disobedience to the authority.

[61] Machine translation of respective provisions by a neural machine translation service.

- Portugal: Article 14.1 of the Cybercrime Law establishes an obligation for any person to communicate or to allow access to data to the criminal justice authorities, if requested.

- Romania: Voluntary cooperation is sought in practice and rendered.

- Senegal: The CPC provides for requiring all persons with knowledge of the functioning of the system or the security measures that protect the data to provide all information necessary to execute the search or seizure. The CPC also permits the authorities to require all persons in possession or control of data to protect its integrity.

- Slovenia: Article 219a of the CPC obliges owners or users of electronic devices to provide access to the item, encryption access keys or passwords, and any necessary explanations about the functioning of the item.

- Spain: Article 588e(c) 5 of the CPC empowers authorities and agents responsible for investigations to order a person to provide the necessary information.

- Switzerland: Certain third parties may be required to provide information upon request by the authorities. An article of the CrimPC (Art. 265) provides for certain duties to hand over items or assets and provides exceptions from this rule.

- Tonga: Section 9 of the Computer Crimes Act allows a magistrate to issue a warrant that covers the provision of necessary assistance and Section 10 provides for sanctions.

- Türkiye: The prosecutor's office is authorised under Article 160-161 of Turkish Criminal Procedure Code to order the production or protection of data.

- United Kingdom: Part III of the RIPA 2000 provides for powers to require protected electronic information which they have either acquired lawfully or are likely to obtain lawfully, to be put into an intelligible form.

- USA: competent authorities can obtain court orders under the All-Writs Act, 28 U.S.C. § 1651, to order a third party to provide assistance with the execution of a search warrant under certain circumstances if needed.

7.2 Implementation of Article 19.4 – Assessment

Answers to the following question of the questionnaire was assessed:

- 2.4.1 Please summarise what legislative or other measures your country has undertaken to ensure that your authorities are able to order a person to provide necessary information as described in Article 19.4. Please summarise the rules applicable to this provision.

Party	Legislative and other measures	Assessment
Albania	Albania indicated that Article 208/a of the CPC provides that the prosecution may appoint an expert who knows the functioning of the computer system or of the measures applied to protect computer data, to enable the measures provided for in this Article. Albania clarified that this provision should not be understood as limited exclusively to experts and may be interpreted as meaning that the prosecutor may order any person with specific knowledge of the functioning of a computer system.	Albania applies specific search and seizure powers to implement Article 19.4. However, a more specific wording in the domestic law of Albania containing all elements of Art. 19.4. could permit greater clarity and enhance legal certainty.
Andorra	Two articles of the criminal code penalise the failure to follow the order of a judge or other public authorities. Information provided by a person with knowledge about the system or its protections will go either to the judge or to the specialised police, as appropriate.	Andorra applies general powers to implement Article 19.4. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.
Argentina	In its response, Argentina does not mention any provision that expressly contains the specific power provided for in Article 19.4 of the Convention, furthermore, it is stated that this provision has not been implemented in Argentina and the authorities rely on general powers provided for in domestic law. However, since the provinces have the capacity to regulate their local procedural codes, it was further reported that the Criminal Procedural Code of Neuquén provides that "Any natural or legal person that provides a remote service by electronic means may be required to hand over information in its possession or control regarding users or subscribers, or their data. The information that is not useful to the investigation may not be used and must be returned, prior to being made available to the defense, which may request its preservation. The limitations applicable to documents shall apply.	Argentina applies general powers to implement Article 19.4. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.

Party	Legislative and other measures	Assessment
Armenia	Armenia stated that it has put in place legislative and other measures to permit the authorities to order persons with knowledge about the functioning of a system or the measures applied to protect data to provide necessary information. Armenia quotes Art. 232 of the CPC that allows investigators to ask any organization for important details related to the case. Authorities state that under the approval of the supervising prosecutor, investigators may also request for example details such as when and for how long someone connects to the internet, their internet protocol (IP) address, and other personalization data related to internet.	Armenia applies general search and seizure powers to implement Article 19.4. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.
Australia	Per the two relevant statutes, court orders may require a specified person to provide any necessary information or assistance to the officers executing the search.	Australia applies specific search and seizure powers to implement Art. 19.4.
Austria	Section 111 of the CCP requires persons with objects or assets in their control to assist the authorities (with certain limitations). Section 93 of the CCP specifies when coercive measures and findings of contempt are available if relevant persons fail to assist.	Austria applies a combination of general and specific powers to implement Article 19.4.
Azerbaijan	There are no specific provisions regarding requiring persons to assist investigations as in Article 19.4, but, in practice, the general provisions for evidence collection and investigative procedures apply to fulfil the requirements of 19.4. Articles 245.6, .7 and .9 permit investigators to impound or search for objects that are not voluntarily surrendered. Investigators may also open closed buildings or storerooms if they are not voluntarily opened. These provisions provide a legal framework to compel individuals to provide necessary information relevant to investigations, including regarding the functioning of systems and measures applied to protect electronic data. The authorities typically rely on these general norms in electronic cases.	Azerbaijan applies general search and seizure powers to implement Article 19.4. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.
Belgium	Article 88quater provides that a juge d'instruction may order necessary cooperation (other than from the defendant and relatives) in the case of an information system, including to turn on a system, locate certain files, reveal access methods, and so on.	Belgium applies specific powers to implement Article 19.4.
Bénin	In general, police requests or orders from the juge d'instruction per the CPC are the basis for obtaining the necessary information. Persons providing such information are legally protected (if they are not themselves implicated in the crime).	Bénin applies a combination of general and specific powers to implement Article 19.4.

Party	Legislative and other measures	Assessment
	In addition, Article 588 of the digital code act requires persons with knowledge of the measures used to secure the system to assist searching officers. Failure to assist is punishable by a fine. Art. 13, 14 and 40 of the CPC, which provide for the powers of the judicial police and public prosecutors, are also applicable.	
Bosnia and Herzegovina	Bosnia and Herzegovina relies on standard CPC rules – legal forms of compulsion, such as subpoenas - to obtain information from witnesses – as well as statutory provisions. Articles 51 and 65 of the CPC require system users to allow access to devices, to produce them and to provide information about them, on pain of potential criminal punishment, including imprisonment. On the opposite side, the codes of Federation Bosnia and Herzegovina, Brcko District, and Republika Srpska, the laws states that those who are using devices must enable access to them, and hand over those storage media. If they don't do it, penalties, fines, or imprisonment will apply.	Bosnia and Herzegovina applies general search and seizure powers to implement Article 19.4. It is not clear that it has the power to require assistance from any person (not merely system users). Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.
Brazil	Courts may compel anyone to collaborate with the Judiciary in discovering the truth. In the event of non-compliance, the judge may order, in addition to imposing a fine, other inductive, coercive, mandatory, or subrogation measures. Legal basis for this can be found in Art. 378-380 of the Code of Civil Procedure. More specifically, pursuant to Art. 378 of the Code of Civil Procedure "no one is exempt from the duty to collaborate with the judiciary in discovering the truth." This provision provides a legal basis for the application of Art. 19.4 under domestic law. On several occasions, the Judiciary has responded to requests from the Federal Police and ordered the temporary suspension of internet service providers' activities and the payment of fines, in order to comply with court orders to provide requested information necessary for ongoing criminal investigations. In this sense, if there is recalcitrance from the system administrator regarding providing access or assisting in conducting the search and seizure, this can be considered a violation of the judicial order that determined the measure, which can even lead to the criminal liability of	Brazil applies general powers to implement Article 19.4. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.

Party	Legislative and other measures	Assessment
	the administrator or whoever holds the necessary information and refuses to provide it in the interest of executing the precautionary measure. In practice, Brazilian authorities can order anyone with knowledge about the functioning of the computer system or measures applied to protect computer data to provide the necessary information. However, the provision of this information is restricted to what is "reasonable." In some circumstances, it may include disclosing a password or another security measure. However, in other situations, this may not be reasonable, such as when the disclosure would threaten the privacy of other users. In these cases, the "necessary information" could be the disclosure of the actual data being sought by the competent authorities, in an intelligible and readable format.	
Bulgaria	Generally, each and every person is obliged by law to cooperate with the investigation authorities and to share everything he/she knows when questioned. According to Article 4 of the Law on the Ministry of Interior: State authorities, organizations, legal persons and citizens shall be obliged to provide assistance to and observe the orders of the MoI authorities issued during, or in connection with, the fulfilment of their statutory functions. Article 64 of the same law provides that police authorities may issue written orders to organizations, legal persons and citizens when needed for fulfillment of police functions. These orders are compulsory unless they require the performance of an obvious crime or violation or endanger the life or health of the person concerned. Article 159 of the CPC may also be relevant, since (pursuant to a request by a court or certain authorities) all establishments, juridical persons, officials and citizens must produce objects, papers, computer information data and other data that may be important to a case.	Bulgaria applies general powers to implement Article 19.4. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.
Cabo Verde	Cabo Verde informed that Article 16 of the CL allows for injunctions to be issued to those who have control or availability of data. The legislator provided this possibility while still within the scope of the law. The article states: If it becomes necessary to produce evidence during the process to discover the truth and obtain specific computer data stored in a particular system, the competent judicial authority can order the person who has control or availability of the data to make it available for the process or allow access to it. Failure to comply with this order may result in punishment for disobedience. Also, whoever has availability or control of these data must comply with the order described in paragraphs 1 and 2. They must make these data available to the competent judicial authority or allow access to the computer system	Cabo Verde applies specific search and seizure powers to implement Article 19.4., however it appears that the scope of the measure under domestic legal framework applies to narrower category of persons than those under Art. 19.4".

Party	Legislative and other measures	Assessment
	where they are stored, under penalty of punishment for disobedience. However, there are limits to the use of such an injunction. It cannot be applied to computer systems used for legal, medical, banking, or journalistic activities. Instead, the secrecy regime for professionals, functions, and state secrets outlined in Article 247 of the Criminal Procedure Code must be applied with necessary adaptations. Additionally, this injunction cannot be directed at a suspect or defendant in the case.	
Cameroon	Article 55 of Cameroon's cybercrime law allows the authorities (state counsel, juge d'instruction or the competent court) to request any qualified natural person or corporate body to perform technical operations to obtain the plaintext version of seized data when it appears that data seized or obtained during an investigation or inquiry has been encrypted.	Cameroon applies specific search and seizure powers to implement Article 19.4., however it appears that the scope of the measure under domestic legal framework applies the measure covers a narrower type of situations and a narrower category of persons than those under Article 19.4. of the BC.
Canada	Section 487.02 of the Criminal Code provides that a court issuing a warrant may order a person to provide assistance to a search, if the person's assistance may reasonably be considered to be required. Section 487(2.2) explicitly provides (in several subparagraphs) that a person in charge of a building or location may be required to permit access to and retrieval of data.	Canada applies a combination of general and specific search and seizure powers to implement Article 19.4.
Chile	Replies provided by Chile indicate that the legislation in this regard consists of Article 12 of Law 21,459, in conjunction with Articles 222 to 226 of the Criminal Procedure Code. Chile also quotes Art. 190 of the CPC through which the prosecutor may summon different people as witnesses to take statements.	Chile applies general search and seizure powers to implement Article 19.4. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.
Colombia	Colombia indicated that under Colombian law, persons who know the operation of a system must appear and collaborate with the authorities in the process of evaluating and extracting information in a manner that is effective and simple.	Colombia applies general search and seizure powers to implement Article 19.4. Provisions specific to computer

Party	Legislative and other measures	Assessment
	To this end, the Judicial Police and the Prosecutor of the case can summon them to appear in the process as witnesses through an interview or a declaration under oath; their knowledge of the system and the data stored there, as well as its structure, format, and location, are valued as an element of conviction when establishing reasonable grounds for obtaining digital evidence and have the potential to be witnesses in the process. On the other hand, in Colombia, there is a duty to cooperate with the authorities as dictated by Article 4 of Law 62 of 1993, which in turn is limited by Article 33 of the Political Constitution of Colombia which states that "no one can be forced to testify against himself, his spouse, permanent partner or relatives within the fourth degree of conscience, relatives within the fourth degree of consanguinity, second degree of affinity or first civil degree".	data and systems could permit greater clarity and enhance legal certainty.
Costa Rica	A Judge based on article 7 of the Organic Law of the Judicial Power (Law 8 of 1937) could order any person to help with the investigation according to their field of knowledge and that person MUST comply with the order. This does not apply if the person with the specific knowledge or information is the defendant itself. In this case, he/she could deny the request based on their constitutional right of no auto-incrimination. The article that regulates it stipulates the following: Article 7: In order to carry out resolutions or perform the actions they order; the courts may request the assistance of the police force and other appropriate means of action. Individuals are obligated to provide the assistance that is requested of them and that they can provide.	Costa Rica applies general powers to implement Article 19.4. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.
Croatia	Article 257 of the CPC obliges any person using computers or devices, any person with access to them, or any telecommunications service provider to provide access to the computer, device or data carrier and give necessary information for an undisturbed use and the fulfilment of search objectives However, it seems that the scope of the measure may be applied to a narrower category of persons than Art. 19.4 which is not limited to users of the computers and persons having access, but applies to a broader category of persons who may have useful knowledge. The authorities conducting the search may order a professional assistant to carry out those measures. Failure to comply with these requirements is punishable (with an exception for the defendant).	Croatia applies specific search and seizure powers to implement Article 19.4. It appears that the applicable framework is limited to a narrower category of persons than foreseen by Art. 19.4.

Party	Legislative and other measures	Assessment
Cyprus	It was reported that police officers have the power to interview any person with information relevant to a case, including those with the types of knowledge described in Art. 19.4. However, based on Cyprus' supplemental responses, it appears that Article 19.4 of the Budapest Convention is normally not implemented and that searches are conducted in reliance on other mechanisms. Generally, during the search of a location, law enforcement does not cooperate with or request the assistance of private system administrators or, apparently, other categories of persons. Searches for electronic data are usually executed by police officers and members of the Digital Forensic Lab (DFL) of the Cyber Crime Unit. During the execution of the search warrant, a preliminary search might be done at the searched location on the electronic data found, but more-extensive examination of the data is done at the Digital Forensic Lab. In special or large-volume cases, members of the DFL remain at the scene during the forensic acquisition of the data. In such cases, the law enforcement agents and DFL carry out the searches without the assistance of outside systems administrators. This is because of the strict nature of the search and the protections of private life and private communication afforded by the Constitution. If the search is done on businesses or organizations that employs a system administrator, during the search, the members of the DFL will usually ask for the sysadmin's cooperation. Failure to cooperate is not a criminal offence and cooperation cannot be compelled. Outside experts may be used to examine the evidence after the search and seizure, but this is usually done in exceptional cases when the DFL cannot further examine the collected evidence e.g. heavily damaged electronic data.	It appears that Art. 19.4 is not implemented into domestic law of Cyprus.
Czech Republic	According to provision 8 of the CPC it is possible to request cooperation from physical and legal persons and to impose a fine in case of not obeying such request (provision of 66 of the CPC and 36 of the Act on criminal responsibility of legal persons). Such obligation is limited in some extent by right against self-incrimination.	Czech Republic applies general search and seizure powers to implement Article 19.4. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.

Party	Legislative and other measures	Assessment
Denmark	When the Budapest Convention was implemented in Danish law, Article 19.4 was evaluated as being satisfied by the Danish rules on witnesses, including the means of compelling the attendance of witnesses, and Section 747 of the AJA. According to that section, court approval (via a hearing) may be sought for measures that require the court's assistance or to secure evidence which may be lost, which will be unavailable without significant inconvenience or delay, or which is important to the case or is of public interest. Under Section 804 of the Act, a court may order a person with access to documents or objects that can serve as evidence, to show them or hand them over (except in certain cases). The rules on interference with correspondence can also be used in order to gain the assistance of the service provider.	It appears that Denmark applies general search and seizure powers to implement Article 19.4. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.
Dominican Republic	The Dominican Republic informed that the Public Prosecutor's Office has the power to order the person who knows about the operation of an information system or any of its components or of the data protection components or the data protection measures in such a system to provide the necessary information for the information necessary to carry out the necessary investigations (article 54 of law 53-07).	Dominican Republic applies specific search and seizure powers to implement Article 19.4.
Estonia	The suspect and accused have their procedural rights and cannot be compelled to assist. However, often these persons cooperate with the authorities and provide information, access to computer systems etc. In case a person can be considered as a witness, then he/she has obligations to provide information. Law enforcement authorities can also involve their experts and bring them to the location where the search takes place. According to Article 95 of the CPC, an expert is "a person who applies non-legal specialised knowledge when conducting an expert assessment in situations and following the rules provided by this Code." When experts are designated, preference is normally given to an employee of a government forensic agency, but private or foreign experts may also be selected.	Estonia applies general search and seizure powers to implement Article 19.4. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.
Fiji	Under sections 20, 21(1) (2) (3) (4) of TCA, the judge issuing the warrant authorizing police or an authorized person (with assistance) to seize or secure a specified computer system, program, data, or data storage medium; inspect and verify the operation of any computer system outlined in the warrant; require any person possessing knowledge about the functioning computer system or measure applied to protect the computer data therein to provide, as is reasonable, the necessary computer data or information, to enable the police/authorized person to conduct such activities as authorized; Request access to any decryption information needed to decrypt data relevant to the warrant and finally, obtain reasonable technical or other assistance to carry out the activities specified in the warrant.	Fiji applies specific search and seizure powers to implement Article 19.4.

Party	Legislative and other measures	Assessment
	Provisions of Criminal Procedure Act on service of search warrants and powers of magistrate, as well as Constitution of Fiji (Section 24) and Police Act are also applicable in this respect.	
Finland	Chapter 8, Section 23 of the CMA stipulates the obligation of a person who possesses an information system to provide information. A person who owns or maintains an information system or any other person shall, upon request, provide a criminal investigation authority with the passwords and other related information necessary to conduct a search of the data contained in a device. Upon request, a written certificate shall be provided to the person to whom the request is made. If a person refuses to provide the information, he or she may be heard in court in the manner provided for in Chapter 7, Section 9 of the Criminal Investigation Act (805/2011). The above provisions do not apply to the suspect of the offence or to a person referred to in Chapter 7, Section 3, Subsection 1 or 2, who has the right or the duty to refuse to testify. The amendments to the CMA entered into force on 1 October 2023 (Act 452/2023) Section 23 now mandates that individuals possessing or maintaining information systems must not only provide passwords and necessary information to law enforcement but also assist in using this information. In addition, the provisions of Chapter 8, Sections 23 to 26 on the obligation of the person possessing an information system to provide information and on the data retention order shall apply to the use of covert coercive measures.	Finland applies specific search and seizure powers to implement Article 19.4.
France	The CPC provides that the police may require the assistance of persons with information about a system. In particular, two offences created in recent years specifically target the refusal to assist with decryption. It seems that the scope of the provision is narrower than Art. 19.4, as they concern decryption matters, whereas Art. 19.4 covers provision of necessary information.	France applies specific search and seizure powers to implement Article 19.4. However, it appears that the applicable domestic law provision is narrower than Art. 19.4.
Georgia	According to Art. 112 of the CPC, investigators and/or other law enforcement officers executing a search warrant must first offer the persons responsible for the search site (usually, homeowners, or in case of companies, managers, system administrators etc) to voluntarily produce data or hand over items to be searched and seized. Per a court order founded on Article 136 of the CPC, a system administrator or any other relevant person under Article 19.4 of Budapest can be ordered to disclose pertinent information to facilitate a search and seizure. Failure to comply with such a court order may give rise to criminal liability under the criminal code.	Georgia applies specific search and seizure powers to implement Article 19.4.

Party	Legislative and other measures	Assessment
	Authorities refer also to Art. 114 of the CPC, which can be extended to non-cooperative managers or system administrators but point out that it is not used in practice very often.	
Germany	Germany does not have a provision that contains expressly the power provided for in Art. 19.4. However, in practice, it is understood that the general provisions of Section 94 and 95 are applicable. According to Section 95 (1) of the Code of Criminal Procedure, only persons who are not suspected of any crime could possibly be obliged to hand over access codes or talk about their knowledge about the functioning of a computer system. Suspects or persons entitled to refuse to testify, on the other hand, cannot be obliged. In such cases, access codes could – if available – be collected from telecommunications/tele media service providers pursuant to Section 100j (1) sentences 2 and 3 of the Code of Criminal Procedure. Law enforcement authorities could furthermore attempt to decrypt access codes, if necessary, with the involvement of specialists.	Germany applies general search and seizure powers to implement Article 19.4. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.
Ghana	Pursuant to Section 99(2) of the ETA, law enforcement officers executing warrants under the Act may require any person in charge of, or otherwise concerned with, the operation of a computer to provide the officer or any other authorised person with reasonable technical and other assistance necessary for the investigation or prosecution. Further, a person in possession of decryption information may be required to provide to officers acting under this section any information necessary to decrypt a record required for the investigation. Persons may also be required to produce computers to officers. Section 98(1) of the ETA allows law enforcement to use the provisions on search and seizure in the ETA to be used in addition to the powers of arrest, search and seizure of a law enforcement agency provided by other statutes. Accordingly, a third-party assistance supported by the ETA may be used in addition to powers under other statutes. A person who refuses to provide assistance when a lawful order has been issued may be sanctioned.	Ghana applies a combination of general and specific search and seizure powers to implement Article 19.4.
Greece	There is no provision for requiring a person to provide information about a computer system.	It seems that Art. 19.4 has not been implemented by Greece.

Party	Legislative and other measures	Assessment
Grenada	Section 22 letter d) of the Electronic Crimes Act requires a person in possession of decryption information to provide the police with access to such decryption information as is necessary to decrypt data required for investigating the offense. The power can be applied to any person who has the responsibility of accessing the system or who has the access code for the system. The functioning or operation of the system is not taken into consideration.	Grenada applies specific powers to implement Art. 19.4. However, it appears that the scope of the applicable domestic legal framework may apply to a narrower category of persons than those under Art. 19.4.
Hungary	Sections 267 and 271 of the CPC establish the power in general for the authorities to collect criminal evidence and to request relevant information from any person (while protecting that person's fundamental rights and ensuring that they are affected only to the extent necessary). Section 305 of the CPC provides that authorities may require a person to make electronic data accessible. Persons who impede searches may be fined. Section 312 of the CPC provides that the possessor or processor of a thing or electronic data can be required to reveal their location or to make electronic data accessible. Failure to comply may lead to a fine (except for persons in certain categories). Under Section 261 of the CPC, certain entities and organisations have special protection from requests for electronic data. In such cases, a prosecutor's authorisation must be obtained. If such authorisation exists, or if the case is urgent enough that the law permits the request without such authorisation, data must be disclosed. Requests without authorisation must be authorised post facto without delay. Data obtained without authorisation are inadmissible at trial.	Hungary applies a combination of general and specific search and seizure powers to implement Article 19.4.
Iceland	In Article 92 of the Act no. 70/2022 on Electronic Communications obligations are laid upon telecommunication companies to assist the police in criminal investigations when the police request assistance.	Iceland applies specific search and seizure powers to implement Article 19.4. However, the applicable provision of the domestic law appears to be narrower than Art. 19.4. since it covers solely telecommunication companies.
Israel	Article 45 of the Criminal Procedure Ordinance requires the occupant of the place for which a search warrant has been granted to provide entry and any reasonable assistance. This article can be interpreted as applying, with appropriate changes, to a computer search. There is no case law on this issue.	Israel applies general search and seizure powers to implement Article 19.4. Provisions specific to computer data and systems could permit

Party	Legislative and other measures	Assessment
	If knowledge about a computer system is in the form of a document, competent authorities can apply for a warrant under Article 43 of the Criminal Procedure Ordinance. Such a warrant requires any person to provide documents relevant to an investigation.	greater clarity and enhance legal certainty.
Italy	**Article 351(1)** is generally applied. The Italian Criminal Procedure Code includes the following articles: **Art. 256 - Production Order**: People mentioned **in articles 200 and 201 are obligated** to promptly provide the judicial authority with documents, deeds, data, information, computer programs, and any other relevant materials related to their profession, job, ministry, or art. This should also include original copies if required, unless they declare in writing that it involves a State secret or a professional or office-related secret. If a declaration pertains to official or professional secrecy and raises doubts about its validity, the judicial authority may conduct necessary investigations. If the declaration is found to be unfounded, the judicial authority can order seizure. In cases of a declaration related to a State secret, the judicial authority informs the President of the Council of Ministers, seeking confirmation. If the secret is confirmed and the evidence is crucial for the trial, the judge may rule that it is unnecessary to proceed due to the existence of a State secret. If the President of the Council of Ministers fails to confirm the secrecy within sixty days of notification, the judicial authority can order seizure. Article 204 provisions apply. **Art. 234-bis - Acquisition of Documents and Computer Data:** The acquisition of documents and IT data stored abroad, even those not publicly available, is always permitted, provided there is consent from the legitimate owner in the case of non-public data. **Art. 248 – Request for delivery** If a IT data is sought through search, the judicial authority may require its delivery through Art. 248 that provides for delivery of objects. In order to be trace the IT data to be seized, the judicial authority or the criminal police officials (delegated by the judicial authority) may examine documents and correspondence as well as data, information and software in banks.	Italy applies general search and seizure powers to implement Article 19.4. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.

Party	Legislative and other measures	Assessment
	Additionally, authorities may apply Art. 351 that provides for other types of investigative questioning.	
Japan	Articles of the CPC permit the authorities to require persons to assist the search or seizure, in particular to operate the computer or to copy and transfer data, and to cooperate in other ways.	Japan applies a combination of general and specific search and seizure powers to implement Article 19.4.
Kiribati	Section 24 of the Cybercrime Act provides that a court may order persons or providers with possession or control of a computer system to assist law enforcement with a search. A police officer must satisfy the court that the targeted data is required for the purpose of a criminal investigation or criminal proceedings.	Kiribati applies specific search and seizure powers to implement Article 19.4. It is not clear that Kiribati has the power to compel assistance from anyone with knowledge (rather than possession or control) of a system. Articles 23 and 24 do not seem to cover this, but the power may be elsewhere in Kiribati law.
Latvia	According to Article 190 of the CPC, the authorities may obtain electronic information from persons affected by searches and seizures. The authorities have additional powers when they are acting per Article 219, special investigative actions. However, the CPC does not provide for sanctions against persons who do not cooperate in ordinary searches and seizures (and potential defendants have protections against self-incrimination that permit them to decline cooperation).	Latvia applies specific search and seizure powers to implement Article 19.4., however the CPC does not provide for sanctions against persons who do not cooperate.
Liechtenstein	Several sections of the CPC provide for requiring persons to assist in a seizure and to compel such assistance if it is refused. Importantly, such persons must turn over storage media and any access mechanisms and provide data in a common format if necessary. Refusal to assist may be punished by fines or imprisonment.	Liechtenstein applies a combination of general and specific search and seizure powers to implement Article 19.4.
Lithuania	Article 97 of the CPC states that natural and legal persons must produce objects and documents relevant to the investigation. According to Article 155 of the CPC, a prosecutor's substantiated decision, confirmed by a court, will permit	Lithuania applies general search and seizure powers to implement Article

Party	Legislative and other measures	Assessment
	the prosecution to obtain all the data reasonably necessary for a criminal investigation, including information about the operation of computer systems. Persons who do not comply with such orders may be held liable.	19.4. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.
Luxembourg	Article 66 paragraph 4 of the CPC explicitly allows an investigating judge who has issued a "substantiated order" to require any person (other than the person under investigation) with knowledge of the system or its protections to provide access to 1) the seized system and 2) the seized data in that system or another connected system as well as to provide assistance in understanding protected or encrypted seized data. This provision is subject to certain other articles.	Luxembourg applies a combination of general and specific search and seizure powers to implement Article 19.4.
Malta	Pursuant to Chapter 9 Article 355AD of the Criminal Code -*'Any person who is considered by the police to be in possession of any information or document relevant to any investigation has a legal obligation to comply with a request from the police to attend at a police station to give as required any such information or document.'*	Malta uses general search and seizure powers to implement Article 19.4. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.
Mauritius	Section 28 duplicates Article 19.4. Beyond this, officials applying to judges for orders sometimes include the relevant language in the applications.	Mauritius applies specific search and seizure powers to implement Article 19.4.
Monaco	The Public Prosecutor may require any person with knowledge of the operation of an information system to provide the information necessary to access the data (art. 255 CPC). In addition, the law allows investigators to require the assistance of witnesses, experts, or persons with specific knowledge. Examples include service providers or IT staff (inside or outside a business).	Monaco applies a combination of general and specific search and seizure powers to implement Article 19.4.
Montenegro	Art. 83.3 obliges anyone who is in possession of objects that can be used as evidence in criminal proceedings to l hand them over. Art. 83.4 extends the application to data saved in devices for automatic or electronic data processing and media wherein such data are saved, which shall, upon the request of the court, be handed over in a legible and comprehensible form.	Montenegro applies a combination of general and specific search and seizure powers to implement Article 19.4

Party	Legislative and other measures	Assessment
Morocco	Licensed public telecommunications networks and service providers are obligated to assist the judicial authorities. However, this obligation does not seem to extend beyond such networks and providers to other persons and entities. However, it should be noted that Morocco is in the process of updating its legislation. In the meantime, its criminal procedure mechanisms are close in practice to the requirements of the Convention.	Morocco applies general search and seizure powers to implement Article 19.4. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty. It appears that the applicable provision under domestic legal framework applies to narrower category of persons than those under Art. 19.4.
Netherlands	In the Netherlands, Article 125k DCCP grants the authority to issue an order for the removal of a security measure (Art. 125k, paragraph 1 DCCP) and to issue an order for the decryption of, or the surrender of a decryption key for, encrypted data (Art. 125k, paragraph 2 DCCP). In such cases, if requested, the individual to whom the order is directed must comply by providing their expertise in security. The decryption order is applicable only to security measures implemented by the natural or legal person. These orders may not be issued to suspects due to the prohibition of self-incrimination. An extra element of information could be to elaborate on the power in article 558 DCCP Condoning the (involuntary) breach of biometric security on a computer device - art. 558 DCCP: people can be forced to condone certain "forced actions" for biometric accreditation to open a device that is locked by fingerprint or face ID. People must condone such powers if they can be done without obliging people to wilfully do something themselves. Laying a thumb on the smartphone or bringing the smartphone in front of a person's face can be done without forcing the person to give the credential.	Netherlands applies specific search and seizure powers to implement Article 19.4.
Nigeria	When the ex parte application is made to a court for an order, the requesting officer may ask that the court include that any person must provide information necessary to the case.	Nigeria applies a combination of general and specific search and seizure powers to implement Article 19.4.
North Macedonia	Several CPC articles cover persons who use or have access to computers, devices, etc., and require them to "give all necessary information required for unobstructed fulfilment of the goals of the search." This definition covers those most	North Macedonia applies a combination of general and specific

Party	Legislative and other measures	Assessment
	likely to have useful search information but does not extend to anyone else who might, in a given case, have search-related information – a friend of the target, someone who works in a building but not with the computers, etc.	search and seizure powers to implement Article 19.4. It appears that the applicable domestic law applies to narrower category of persons than those under Art. 19.4.
Norway	Section 199a of the CPC provides for requiring the assistance of anyone involved with the targeted system.	Norway applies specific search and seizure powers to implement Article 19.4.
Panama	Article 75 of the Criminal Procedure Code establishes the obligation to cooperate, applicable to both public and private entities, in a prompt, effective and complete manner to the requirements formulated by the agents of the Public Prosecutor's Office. In addition, Article 277 of the same legal excerpt establishes that, given the urgency and purpose of the process, information may be requested from any public servant, who is obliged to provide it and collaborate with the investigation. It also establishes that information held by both natural and legal persons may be requested. Article 75. Obligation to collaborate. Public and private entities are required to provide prompt, effective and complete collaboration to the requirements formulated by the agents of the Public Prosecutor's Office in compliance with their functions, under penalty of incurring the responsibilities provided for by law. The agents of the Public Prosecutor's Office shall have the coercive powers conferred on them by this Code, its Organic Law or special laws. Art. 277. Collaboration with the Public Prosecutor's Office. Apart from the cases that require the authorisation of the judge, the Public Prosecutor's Office, considering the urgency and purposes of the process, may request information from any public servant, who is obliged to provide it and to collaborate with the investigation according to his competence. It may also request information held by natural or legal persons.	Panama applies general search and seizure powers to implement Article 19.4. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.
Paraguay	There is no specific provision expressly providing for the power of art. 19.4 and its application by the authorities arises from practice.	It appears that authorities rely solely on practice and on general powers to implement Article 19.4. Provisions specific to computer data and

Party	Legislative and other measures	Assessment
	The authorities informed that there are only good practices and requests based on the search for evidence that involves cybercrimes of law 4439/2011 and the Budapest Convention.	systems could permit greater clarity and enhance legal certainty.
Peru	The Peruvian legal system grants authorities the power to demand necessary information from individuals during an investigation. The Public Ministry, according to the b) of numeral 3 of article 337 of the Criminal Procedure Code can request information from any person and even seize private documents if necessary. Failure to comply with these requirements may lead to criminal charges for resistance or disobedience to authority, as specified in Article 368 of the Criminal Code. Furthermore, both the Prosecutor and the Judge, as stated in Article 126 of the Criminal Procedure Code, have the authority to use force to fulfil their duties if required.	Peru applies general search and seizure powers to implement Article 19.4. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.
Philippines	The Cybercrime Prevention Act specifically provides that any person with knowledge about the functioning of a computer system and measures to protect and preserve its data may be ordered to provide, as is reasonable, information to assist searches, seizures and examinations.	The Philippines applies specific search and seizure powers to implement Article 19.4.
Poland	Per Article 175 of the CPC, suspects and accused persons cannot be compelled to assist, although they often choose to do so. Anyone who may be considered a witness may be compelled to assist. The search supervisor decides who will be considered a witness to be questioned. Sanctions may be imposed on a witness for failure to provide information. It is not clear whether the ability to question a "witness" means that a person at the site of a search may be required to provide information immediately.	Poland applies general search and seizure powers to implement Article 19.4. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.
Portugal	There is no express statutory provision allowing the authorities to order a person's assistance. However, Article 14, paragraph 1, of the Cybercrime Law effectively implements Budapest Article 19.4. Article 14 is designed primarily to transpose Budapest Article 18 (production orders) into domestic law; therefore, it creates an obligation for any citizen to communicate certain data to the criminal justice authorities, if requested (with the exception of persons in certain protected categories). Under this article, a person may be required to "allow access to data" in search cases, if necessary. Refusal to allow access to the data can be charged as the crime of disobedience, with a corresponding criminal sanction.	Portugal applies specific search and seizure powers to implement Article 19.4.
Republic of Moldova	Per Articles 300-306 of the CPC, every natural person or legal entity must comply with court orders, including orders to provide information or evidence. Computer data constitutes evidence.	Moldova applies general search and seizure powers to implement Article 19.4. Provisions specific to computer

Party	Legislative and other measures	Assessment
		data and systems could permit greater clarity and enhance legal certainty.
Romania	There is no provision to compel a person to provide technical support prior to or during a computer search. However, in practice voluntary cooperation is sought and rendered. The subject of the search or the owner, perpetrator, witness, and relatives of the perpetrators have the right to decline to cooperate in a criminal case, based on different principles, such as the right not to incriminate themselves.	Romania has not implemented Art. 19.4.
San Marino	San Marino does not have specific legislation on the subject, but it was indicated that if it is suspected that data or information useful for conducting criminal investigations are contained in a computer or telematic system, or in a part of it, and there are reasonable grounds to believe that such data may be lost or deleted, the Judge, by means of a reasoned decree, may order the person who controls such data or information, or who has them available, to take the necessary technical measures to ensure the immediate protection and preservation of the original data. Furthermore, the judge may order the person to whom the decree is addressed to take all necessary measures to ensure the confidentiality of the data. If it is suspected that data or information useful for carrying out criminal investigations is contained in a computer or telematic system, or in a part thereof, the Judge, by means of a reasoned decree, may order the person who controls such data or information, or whoever has it available, to transmit it to the Judicial Authority. Authorities reported also the possibility of requesting the preservation of data useful for the investigation. The Judge, by reasoned decree, may order the person who has the availability or control of the data to adopt the appropriate technical measures to ensure the timely protection and preservation of the data in their original state; however, there is no legislative definition of "computer system administrator". There is also no regulation allowing the Judicial Authority to oblige such a person, who is aware of the functioning of the system or of the data protection measures, to provide assistance or information necessary to carry out searches or seizures.	San Marino applies general powers to implement Article 19.4. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.

Party	Legislative and other measures	Assessment
Senegal	The CPC articles cited above provide for requiring all persons with knowledge of the functioning of the system or the security measures that protect the data to provide all information necessary to execute the search or seizure. Those articles also permit the authorities to require all persons to protect the integrity of the data in their possession or control.	Senegal applies specific search and seizure powers to implement Article 19.4.
Serbia	Pursuant to the CPC, the Law on Public Prosecution and, in certain cases, the Law on Electronic Communication, all legal and natural persons (with the exception of suspects/defendants) are required to assist investigations as described in Article 19.4.	Serbia applies a combination of general and specific search and seizure powers to implement Article 19.4.
Sierra Leone	The warrant in Section 10 may authorize a law enforcement officer or other persons possessing knowledge about the functioning of a computer system, or measures applied to protect computer data therein, to provide the necessary computer data or information, to enable an enforcement officer or other authorized person in conducting an activity authorized under the Act.	Sierra Leone applies specific search and seizure powers to implement Article 19.4.
Slovak Republic	The Slovak Republic cites Sections 91.5, 91.6 and 116 of the CPC as the basis for the capacity to order persons to assist with searches. Although it appears that Sections 91.5 and 91.6 may cover some elements of Art. 19.4. of the Convention, the domestic power focuses solely on owners/users of systems and service providers, but it does not seem to be broad enough to capture less-expected categories of people who may have useful knowledge, as required by Art. 19.4.	Slovak Republic applies specific search and seizure powers to implement Article 19.4. However, It appears that the applicable domestic law is narrower than Art. 19.4.
Slovenia	Under Article 219a of the CPC, owners or users of electronic devices must provide access to the item, encryption access keys or passwords, and any necessary explanations about the functioning of the item. Persons who refuse to cooperate may be punished, including by imprisonment (except for persons in certain categories, such as defendants).	Slovenia applies specific search and seizure powers to implement Article 19.4. However, applicable provision under domestic legal framework seems to apply to a narrower category of persons than those under Art. 19.4.
Spain	The Spanish Criminal Procedure Act contains a similar provision in Article 588e(c) 5 to that described in Article 19.4. The authorities and agents responsible for investigations are empowered to order a person to provide the necessary information. This power is not limited to the judicial authority, but also extends to the prosecution and law enforcement	Spain applies specific search and seizure powers to implement Article 19.4.

Party	Legislative and other measures	Assessment
	authorities. Failure to comply with the request may be considered an offense of disobedience. However, persons exempted from the obligation to testify on the grounds of kinship or professional secrecy cannot be sued for failure to cooperate in investigations related to their obligation to maintain confidentiality.	
Sri Lanka	Section 23 of the Computer Crime Act requires persons to comply with lawful requests by experts or police officers during investigations.	Sri Lanka applies specific search and seizure powers to implement Article 19.4.
Sweden	The CPC provides that, if a search would otherwise be obstructed, a person may be required to provide biometric authentication so that a system or device may be accessed. Further, the CPC provides that a person may be required to testify before the court to provide necessary information about a system while a preliminary investigation is still in progress. This testimony may take place only after an investigation has progressed enough that a suspect has been identified, and that suspect has the right to be present at the testimony.	Sweden applies a combination of general and specific search and seizure powers to implement Article 19.4., however it appears that the applicable framework is limited to biometric identifications or witness examination that seem to be narrower and less effective than requirements set out in Art. 19.4.
Switzerland	In certain spheres, the law requires third parties to provide information upon request by the authorities. An article of the CrimPC provides for certain duties to hand over items or assets. However, the provision in the CrimPC primarily addresses the owner of the items or assets to be seized. Furthermore, an accused has the right to refuse to cooperate in a criminal proceeding. Others may be authorised to refuse to testify. Corporate entities do not have to hand over items if they could incriminate themselves such that they could be held liable under criminal or civil law and if their interest in protection outweighs the interest in prosecution.	Switzerland applies general search and seizure powers to implement Article 19.4. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty. It also appears that the applicable domestic law is narrower than Art. 19.4 since it applies to owners of the items or assets to be seized and not to a wider category of persons.

Party	Legislative and other measures	Assessment
Tonga	Section 9 of the Computer Crimes Act allows a magistrate to issue a warrant that covers the provision of necessary assistance by others to law enforcement conducting a search. Perhaps more directly, Section 10 of that act provides criminal penalties for persons in possession or control of data who fail to permit and assist warrant-authorised searches. In addition, if data or information is required for criminal proceedings or investigation, section 11 of the Computer Crimes Act allows a magistrate to order a person in control of a computer system or data to provide them. Additionally, section 15 of the Electronic Communication Abuse Offences Act provides that the Supreme Court can issue a production warrant to allow access to and disclosure of content data and any associated information used in an offence. A magistrate judge may issue such production warrant if the Supreme Court Judge is not available.	Tonga applies specific search and seizure powers to implement Article 19.4.
Tunisia		
Türkiye	Although there is no statutory provision that compels a person to assist, the authorities frequently consult anyone who may have knowledge about the system being searched.	It appears that there is no applicable statutory provision in the domestic law to implement Art. 19.4 and Türkiye relies on practice. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.
Ukraine	Ukraine stated that the current legislation does not provide for separate specific procedural rules that empower the competent authorities to order any person who is aware of the functioning of a computer system or measures taken to protect computer data therein to provide, if reasonable, the necessary information to implement the measures referred to in paragraphs 1 and 2. However, the general procedural rules on the collection of electronic evidence are applicable.	Ukraine applies general powers to implement Article 19.4. Provisions specific to computer data and systems could permit greater clarity and enhance legal certainty.
United Kingdom	Part III of the Regulation of Investigatory Powers Act 2000 (RIPA 2000) seems to provides the statutory framework of general powers applicable to serious crimes, enabling public authorities to require protected electronic information (keys/passwords) which they have either acquired lawfully or are likely to obtain lawfully, to be put into an intelligible form. These powers mean that in circumstances when it is necessary and proportionate to do so, investigators may require companies and individuals who have appropriate permission to provide access to (or the means of access to) protected information which can then be put into an intelligible form.	United Kingdom applies a combination of general and specific powers to implement Article 19.4. However, it seems that the measure covers a narrower type of situations (only keys/passwords after the object

Party	Legislative and other measures	Assessment
	The method of obtaining access to protected information is achieved by the service of a notice requiring disclosure (section 49, RIPA 2000). The notice must be founded on the investigators' belief. Provisions compelling witnesses to attend court hearings and to give evidence at trial may be also used in respective countries.	has already been seized, applying to serious crimes) and a narrower category of persons than those under Article 19.4. of the BC.
United States	Although this is rarely necessary, a court may authorise an order under the All-Writs Act (after application) to compel the type of assistance required by Article 19.4.	The United States applies a combination of general and specific search and seizure powers to implement Article 19.4.

8 CONDITIONS AND SAFEGUARDS (ASSESSMENT OF ARTICLE 19.5)

This section assesses implementation of Article 19.5:

> Article 19 – Search and seizure of stored computer data
>
> 5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

8.1 Implementation of Article 19.5: overview

8.1.1 Conditions and safeguards – summary

Article 19.5 stipulates that the measures in the article are subject to conditions and safeguards provided by the domestic law of the Parties on the basis of Articles 14 and 15 of this Convention.

The assessment of implementation of this provision thus consists of two parts, first related to Article 14 and second to Article 15.

8.1.1.1 Article 14

Article 14 requires Parties to apply the power of search and seizure of stored computer data for the purpose of specific criminal investigations or proceedings to offences established in accordance with the Convention, to other criminal offences committed by means of a computer system as well as to the collection of evidence in electronic form of a criminal offence.

Whether the powers for the search and seizure of stored computer data apply to any offence where evidence is on a computer system (question 1.1.2 of the questionnaire) was already addressed in Section 3.2 of this report and Parties are advised to consult this part for a more detailed discussion. Its most important finding is that almost every Party applies the power of search and seizure of stored computer data to any offence where evidence is on a computer system.

Example of implementation in the domestic law of a Party:

Fiji: *"All powers and procedures under this Act are applicable to and may be exercised with respect to (…) the collection of evidence in electronic form of a criminal offence under this Act or any other written law."*[62]

8.1.1.2 Article 15

Pursuant to Article 15, the Convention's powers and procedures shall be constrained by conditions or safeguards in the domestic law of each Party that balance the requirements of public safety with the protection of human rights and liberties. These conditions or safeguards may be provided constitutionally, legislatively, judicially or otherwise.

The Convention does not specify in detail the conditions and safeguards for each power or procedure since the Convention applies to Parties of many different legal systems and cultures.

On the other hand, the Explanatory Report to the Convention recognises that there are some common standards or minimum safeguards to which Parties to the Convention must adhere

[62] Section 15.c. of the Cybercrime Act.

that arise from obligations that a Party has undertaken under international human rights instruments.[63] However, taking into consideration that Parties from all regions of the world are Parties to the Convention, the drafters did not establish an exhaustive list of such common standards or minimum safeguards; rather, they relied upon citing/referencing human rights treaties.

Equally, the Convention provides that specific safeguards, including judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of a power or procedure, shall apply as appropriate in view of the nature of such power or procedure. For example, the Convention requires its Parties to apply such conditions and safeguards with respect to interception, given its intrusiveness. At the same time, such safeguards need not apply equally to other powers, and Parties may thus decide themselves what they consider "appropriate" with respect to search and seizure of stored computer data. Nevertheless, it is undisputed that search and seizure is a more intrusive procedural measure than data preservation and Parties should introduce more stringent safeguards with respect to search and seizure of stored computer data than those related to expedited preservation of stored computer data.

Given the above, when assessing the effect of Article 15 on the implementation of Article 19.5, the T-CY analysed summaries of domestic law conditions and safeguards provided by Parties as applied to the different measures under Article 19. The focus was to determine whether the powers of search and seizure of stored computer data are subject to conditions and safeguards in the domestic law of each Party, not to assess in detail those safeguards or the lack thereof.

Almost every Party provided information on applicable conditions and safeguards throughout the various parts of the questionnaire. T-CY members are thus advised also to consult previous sections of the report[64] and the compilation of replies, where more detailed answers of each Party appear.[65] The present section thus contains a summary of most common conditions and safeguards referred to by Parties.

It should be noted that almost all Parties reported that they included human rights safeguards and protections when implementing Article 19. Among the most frequently mentioned safeguards was judicial or other independent supervision, while most of the Parties reported court orders or decisions of other judicial authorities as a requirement for authorisation of the power.

A number of Parties emphasised that the procedural powers must respect human rights obligations enshrined in their respective constitutions or fundamental documents. Furthermore, it was pointed out that such powers must be in accordance with Parties' obligations under applicable universal human rights instruments such as the International Covenant on Civil and Political Rights or regional human rights instruments such as the American Convention on Human Rights, the European Convention on Human Rights, or the

[63] See para 145 of the Explanatory Report to the Convention.

[64] For example, Section 3.4 on notification, Section 4.1.5 on competent authorities that authorise and carry out a search, Section 5.1.2 that addresses grounds to believe that data sought are stored in another system in the territory of that Party or Section 6.1.2 on competent authorities that authorise and carry out a seizure.

[65] Parties took different approaches to this question. Some provided wide-ranging answers, beginning with treaties and national fundamental documents and continuing with lists of very specific procedural rights. Other Parties focused more narrowly on practical rights (who must be present at a search?) and procedural rights. Either approach was responsive to the question; Parties simply understood the thrust of the question differently. For this reason, readers should bear in mind that silence about treaties or constitutional rights does not mean that a country does not respect and apply them.

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and its Protocols.

Following are examples of safeguards that were frequently mentioned by Parties:

- legality (the use of all powers must be regulated by law);
- limitation on the scope (e. g. limitation to the specific criminal investigation or proceedings, identification of the known/unknown person whose data is to be accessed, identification of the location or objects to be searched/seized, details on the benefits to the investigation);
- limitation on the duration of the power[66];
- right to a fair trial;
- right to privacy;
- data protection;
- necessity, subsidiarity, proportionality[67] or reasonableness of the measure;
- privileges and immunities (certain categories of individuals or activities may be protected against powers of search and seizure: journalists, journalistic sources, physician-patient conversations, lawyer-client conversations, priest-penitent conversations, diplomats);
- the right against self-incrimination;
- oversight;
- measures related to legal remedies (right to appeal a decision, right of redress);
- measures related to data retention;
- notification of a person concerned by the measure and right to be present at the search.

Several Parties underlined that violation of conditions and safeguards can result in a prohibition of the use of evidence in favour of the person concerned.

Per Article 15.3, the interests of third parties should also be taken into consideration. In relation to this requirement, Slovenia pointed out that the investigation must be carried out in a way that interferes to the smallest possible extent with the rights of persons who are not suspects or defendants, and it must protect the secrecy or confidentiality of data and not cause disproportionate damage.

Other safeguards that were reported were related to the right of a person against whom the measure is taken to be present in a search or a requirement to conduct the search in presence of a number of persons, who are not related in any way with the investigation and are considered impartial (four-eyes principle).

Safeguards related to integrity of the data were mentioned as well. Among them, handling of data in a secure and confidential manner and steps to ensure that the data are not tampered with or altered in any way were among the most quoted. In order to prevent remote access to devices and erasing and/or locking the data, authorities secure portable computers and telephone devices in Faraday's cages or set the devices on aeroplane mode. To achieve this,

[66] With respect to the limitation on the duration of the power, Hungary reported that if the seizure is not necessary any longer for the purposes of a proceeding, arrangements shall be made without delay to terminate the seizure and release the thing seized, or a motion to confiscate the seized thing shall be submitted. Portugal pointed out that all decisions on search and seizure are limited to 30 days, that is, after the judicial authority decision, police have a limited time (up to 30 days), to execute the measure. After that term, the authorisation expires and cannot be executed.

[67] For example, in relation to proportionality, Georgia pointed out that when multiple alternatives are available the least intrusive investigation power should be chosen (e.g. when possible, production of data must be carried out instead of search and seizure).

technical expertise necessary to perform the search, extension of the search, and seizure of stored computer data in a way that maintains the integrity of the data and does not cause undue harm to the system or other data is required.

A few Parties initially reported that in their jurisdictions, there are no applicable conditions and safeguards in relation to search and seizure of stored computer data, however some of them subsequently clarified their replies.

Examples of practices include:

- Australia: obligation to report on the number of warrants

  Agencies must report annually on the number of warrants applied for and issued during the year and the number of emergency authorisations. Records must also be kept about computer access warrants, including in relation to decisions to grant, refuse, withdraw or revoke warrants and how the information in the warrant has been communicated. This allows to review the compliance with the requirements under applicable domestic law.

- Austria: notification in case of seizure

  In all cases of a seizure, a confirmation of the seizure must be handed over to the person concerned immediately or sent within 24 hours at the latest. The confirmation must be in writing and is a (public) document. In any case, the confirmation shall also contain legal notice: It must not only inform about the right to file an objection according to Section 106, but also about the right of the person concerned to apply for a court decision on the lifting or continuation of a seizure (Section 111 para 4 CPC). According to Section 106 para. 1 CPC any person claiming to have their personal rights violated in investigation proceedings by the prosecution authority may raise objections to the court, including if an investigative or coercive measure has been directed or executed in violation of provisions under this Code. The affected person also has the right to apply for a court decision on the lifting or continuation of a seizure according to Section 115 para. 2 CPC. According to Section 115 para. 6 CPC, if and when the prerequisites for seizure fail or cease to exist or if the amount of money is paid, the prosecution authority, or after the indictment has been filed the court, has to lift the seizure. Section 112 CPC also provides for a right of objection in case a person is subject to seizure that enjoys privileges under the CPC (e.g. lawyer/client privilege). In a similar manner, Section 112a CPC foresees conditions and safeguards in regard to specific kinds of classified (intelligence) information. This may, for example, be information that has been transmitted in a classified form by foreign security authorities or security organisations.

- Denmark: addressing privileged data

  Supreme Court decision of 8 January 2015, case 154/2014 (UfR 2015.1249 H). In this case several computers and mobile phones were seized, including the data stored on the devices. Parts of the data material related to the case while other parts were protected by the privilege of information given from sources to media outlets. It was thus decided to mirror the data to a backup, and the court would decide which parts of the data material should be available during the investigation. This process had as its aim to ensure that all relevant data would be part of the investigation while simultaneously protecting the confidentiality between a media outlet and its sources as protected by Danish legislation.

- Netherlands: criteria related to the level of infringement on the privacy with respect to the search of the confiscated computer device (smartphone):

  - When the infringement of privacy is limited: The law enforcement officer may search without further authorisation (Articles 95 and 96 DCCP) (e.g., recently used phone numbers, looking for specific messages or images);
  - When the infringement of privacy is more than limited: prior authorisation of a prosecutor is needed (Article 141 jo Article 148 jo Article 95 or 96 DCCP) (e.g., analysing a copy or image of the contents of the device);
  - When the infringement of privacy is very serious and foreseeable prior authorisation of an investigatory judge is needed. (Article 181 jo. 104 jo. Article 177 DCCP) (no clear examples, but the nature of the stored computer data is considered decisive).

- Sweden: the Commission on Security and Integrity Protection

  A special authority, the Commission on Security and Integrity Protection is tasked with supervising the use by law enforcement agencies of secret surveillance, including secret data interception. The supervision aims in particular in ensuring that the activities are conducted in accordance with laws and other regulations. The Commission exercises its supervision through inspections and other investigations. The Commission may make statements on established circumstances and express its opinion on the need for changes in the activities and shall strive to ensure that any deficiencies in laws and other regulations are remedied. At the request of an individual, the Commission is obliged to check whether an individual has been the subject of secret surveillance and whether the use of secret surveillance and associated activities was in accordance with laws and other regulations. The Commission shall notify the individual that the check has been carried out.

8.2 Implementation of Article 19.5 – Assessment

Answers to the following question of the questionnaire were assessed:

- Conditions and safeguards that are applicable when applying the different measures for the search, extension of the search, and seizure of stored computer data were assessed (answers to question 3.1.1 and other corresponding questions of the questionnaire).

Party	Legislative and other measures	Assessment
Albania	Authorities stated that, these procedural powers are without exception subject to judicial authorisation. According to Article 151 of the CPC, evidence (in general) not obtained by the provisions of the CPC cannot be used in criminal proceedings. It is important to note that paragraph 1 of Article 208/A of the CPC stipulates that this article applies only to information technology crimes.	Albania is partially in line with Art. 19.5. Authorities shall consider extending the scope of the measure to cover all offences where evidence is on a computer system.
Andorra	Authorities indicated that search and seizure of computer data can be applied to all serious criminal offences corresponding to major offences (more than two years' imprisonment), regardless of the nature of the offence, and to minor offences of corruption or influence peddling. Searches must be founded on a sufficient legal basis and be authorised by a juge d'instruction. Such authorisations may be appealed as well as challenged before the constitutional court as violating fundamental rights.	Andorra is partially in line with Art. 19.5. Authorities shall consider extending the scope of the measure to cover all offences where evidence is on a computer system.
Argentina	There are several international treaties on human rights to which Argentina is a party. On the other hand, Article 18 of the National Constitution provides for the inviolability of the home, as well as the inviolability of epistolary correspondence and private papers. In line with this, article 19 of the constitutional text recognizes that "the private actions of men that in no way offend public order and morals, nor harm a third party, are reserved only to God and exempt from the authority of the magistrates...". On the other hand, Argentina has a data protection regime under Article 43 of the National Constitution and Law No. 25,326 on the protection of personal data.	Argentina is in line with Art. 19.5.

Party	Legislative and other measures	Assessment
	It should be noted that, at the international level, Argentina approved the Convention 108+ by means of Law No. 27.699. Access to the contents of cell phones and computers must be carried out by virtue of a court order warrant. The search must have a court order that expressly indicates and justifies the need to access the contents of a certain device. The evidence will not be admitted if it is obtained illegally or in violation of the fundamental guarantees of the criminal process. The regulations and formalities foreseen in an evidentiary means expressly contemplated that can be assimilated to it are applied analogically, provided that constitutional guarantees are not violated.	
Armenia	General conditions and safeguards provided for in the CPC apply to all types of measures, included to search and seizure of stored computer data. These are related to judicial supervision of the measures, actions performed by competent authorities, privileges and immunities, etc.	Armenia is in line with Art. 19.5.
Australia	Numerous avenues for redress are provided by the Crimes Act. They include exclusion of evidence at trial, compensation for damage to equipment, and oversight of decisions and powers by four entities – the Commonwealth Ombudsman, the Australian National Audit Office, Parliament, and the judiciary. Under the SD Act, the first safeguard is that warrants must be issued by a disinterested judge or official. The Act also includes reporting and oversight requirements, including reports to the Attorney General of certain details of each computer access warrant and periodic reports on warrants issued, refused, etc, to the AG and to the Commonwealth Ombudsman.	Australia is in line with Art. 19.5. Authorities should consider extending the scope of the measure to cover all offences where evidence is on a computer system
Austria	Several sections of the CCP ensure the procedural rights of persons affected by a seizure. Written notice of a seizure must be timely provided and include a statement of certain redress rights. Complaints may be directed to the prosecution authority or to the relevant court. If specially-protected data are seized – for example, data subject to the attorney-client privilege – detailed provisions apply, including sequestration of the data, special handling procedures, and so on. Special procedures also apply when classified intelligence information is involved.	Austria is in line with Art. 19.5.
Azerbaijan	Under the CPC, the general provisions applicable to any search and seizure are applicable to electronic searches and seizures as well as to extensions of searches. The relevant CPC articles are subject to Articles 14 and 15 of the Budapest Convention. CPC protections include that searches and certain other investigative acts may be carried out only pursuant to the CPC and based on a court decision. Further, during a criminal	Azerbaijan is in line with Article 19.5.

Party	Legislative and other measures	Assessment
	prosecution, the rights to privacy, confidentiality of communications and inviolability of the person are protected. Any derogation from those rights requires a court decision exception in detention and arrest cases. All investigative acts must be recorded and registered immediately or within a day. All procedural decisions are essential documents that must be recorded on specially-designed forms. No one may enter a dwelling without the consent of those living there except in certain circumstances.	
Belgium	Article 39bis incorporates by reference, and applies to information systems, the general search and seizure rules of the code. The general rules permit complaints by an affected person to the prosecutor. Numerous grounds may be the basis for such complaints, with which the prosecutor may agree or disagree in whole or in part. Appeal beyond the prosecutor's decision is available.	Belgium is in line with Art. 19.5.
Bénin	Generally, calls at a residence and searches may be carried out only between the hours of 6:00 and 21:00, according to the CPC. In addition, the person involved must consent to the search (see above) and the rights of natural persons must be respected in this connection. More specifically, Article 78 of the CPC and Article 592 of the digital code act specify the conditions and guarantees attaching to searches and seizures. Violation of these rules is a basis for nullification of the procedure, however this does not mean that the case is dismissed. For example, failure to comply with the hours of the search constitutes a violation of the suspect's rights by the investigating officer. Generally, the procedure is taken up again and entrusted either to another judicial police unit or to another investigating officer in the same police unit.	Bénin is in in line with Article 19.5.
Bosnia and Herzegovina	The authorities in Bosnia and Herzegovina must comply with numerous safeguards regarding searches and seizures. They include the previously described requirements, such as warrants, as well as protection of the right to a fair trial and to privacy; requirements of necessity, proportionality, and notification; maintaining the integrity of seized data; and nondisclosure of the data to uninvolved persons. Federation Bosnia and Herzegovina mentioned specifically technical measures to preserve the integrity of data.	Bosnia and Herzegovina is in line with Article 19.5.
Brazil	Powers regarding search and seizure apply for criminal offences under domestic law where evidence is on a computer system. This means that if there is evidence of any criminal offense stored on a computer system, whether it is a cybercrime or any other type of crime, the authorities can request a search and seizure of	Brazil is in line with Art. 19.5

Party	Legislative and other measures	Assessment
	the data. The legal framework does not restrict the application of search and seizure powers to specific types of offences. The search, extension, and seizure of stored computer data are subject to safeguards to protect individual rights and privacy while ensuring effective law enforcement. Key safeguards that are provided for in the Brazilian constitution include judicial authorisation based on reasonable suspicion; measures proportionate to the crime being investigated; limitation of the data searched or seized to relevant information; competent authorities with technical expertise; notification to the person whose data are searched; confidentiality of data obtained for investigative purposes only; judicial review of the legality and proportionality of the measures.	
Bulgaria	Relevant safeguards include judicial supervision. Searches are always conducted in the presence of a person who uses the premises or a representative of legal person. A search also always requires the presence of two persons who are not related in any way with the investigation and are considered impartial. Article 137 of the CPC explicitly states the rights and responsibilities of such witnesses: (4) The witnesses of procedural actions shall have the following rights: to make notes and objections on the admitted incompleteness and breaches of the law; to request corrections, amendments and supplementations of the records; to sign the record under special opinion, stating in writing their reasons for this; to require cancellation of the acts, which harm their rights and legal interests; to obtain respective remuneration and coverage of the made expenses.	Bulgaria is in line with Article 19.5.
Cabo Verde	Cabo Verde informed that the competent judicial authority authorises computer searches with a maximum validity of 30 days -under penalty of nullity-, and the authority should oversee the investigation (article 17 of CL). In exceptional cases, the criminal police may conduct searches without prior authorization, such as when consent is provided or in cases of imminent terrorism or organized crime. In this case, the investigation must be detailed in a report that includes the results and evidence, which must be submitted to the judicial authority. In the case of the extension of the search (article 17º, no. 5), the same conditions and safeguards as in article 17 apply, namely, the competent authority, the validity period of the authorization, and the execution	Cabo Verde is in line with Article 19.5.

Party	Legislative and other measures	Assessment
	authorization formalities. A copy of the order ordering the search to proceed will be delivered to whoever has the availability or control of the computer system where the search is intended to be carried out. – article 18º, no. 6, in conjunction with article 237º, of the Criminal Procedure Code. In the case of the computer data seizure (article 18 of CL), if necessary, the seizure must be authorized or ordered by order of the competent judicial authority. The criminal police body may make seizures without prior authorization from the judicial authority, but in this case, it must be during a computer search legitimately ordered and carried out following article 17º (Computer search), as well as when there is urgency or danger in the delay. This situation must be validated within 72 hours. If seizures reveal personal or intimate data, they must be presented to the judge. Seizures related to specific professions are personally overseen by the judge, with prior notification to relevant professional bodies. Searches may be prevented by professional, function, and state secrecy, which can be invoked by designated individuals according to the law.	
Cameroon	Conditions and safeguards applicable in this area derive from the CPC. In addition, other measures will be undertaken regarding the ongoing enforcement of Cameroon's cybercrime framework comprising notably: - the ongoing revision of the abovementioned Cameroon's cybercrime law; - the draft law on the protection of personal data, already drawn up; - the project of a Digital Investigation Procedures Manual.	Cameroon is in line with Article 19.5.
Canada	Two sections of the Criminal Code specify safeguards that relate to search and seizure. These safeguards include that there must be reasonable grounds to believe that an item being sought relates to, or will be used to commit, an offence, or that it will reveal the location of a suspect. If data is seized whose seizure is not authorised by a warrant, it may be excluded as trial evidence. A general warrant may be issued only when a judge is satisfied that (in addition to the usual requirements) the best interests of the administration	Canada is in line with Article 19.5.

Party	Legislative and other measures	Assessment
	of justice will be served by its issuance. Further, a general warrant will not issue unless no other form of warrant or order is applicable to the technique in question. This last requirement ensures that the authorities do not apply for general warrants to evade more-elaborate applications for warrants for specific (electronic) techniques. General warrants are also restricted in other ways. Independent oversight bodies can review, intervene about, and establish guidelines regarding law enforcement practices and procedures. These bodies include the Privacy Commissioner of Canada and parliamentary committees. The Charter of Rights and Freedoms is the overarching guarantor of human rights in this context.	
Chile	The safeguards provided by Article 12 of Law 21,459 include the following aspects: First, the requirement of reasonable suspicion, based on specific facts, of involvement or participation in a criminal act. Secondly, the judge's authorisation is subject to a formal request from the Public Ministry. Finally, the Public Ministry is obliged to provide the judge with an exhaustive and comprehensive report as part of the procedure. The measures provided for in the Code of Criminal Procedure shall be subject to the safeguards set out therein. Safeguards provided for in the Constitution of Chile are applicable as well.	Chile is in line with Art. 19.5.
Colombia	Colombia indicated that the legislation recognizes the protection of privacy and habeas data during the execution of judicial police activities. They also suggested that the provisions and investigative powers in the previous paragraphs apply to i) cases in which hardcore computer-related conduct comparable to articles 2 to 11 of the BC is investigated; ii) conduct in which information technologies have been used as a medium, including computer devices and systems; and iii) any other case in which the collection of digital evidence is required. To ensure the protection of these rights, it provides that: - The written order must be issued by a public prosecutor and must be motivated, must delimit the virtual spaces to be searched, the data to be extracted, and their relationship to the information to be extracted data to be obtained, and its relation to the investigative hypothesis. - Analogously to the application of search warrants in physical spaces, the prosecutor's written order must delimit the virtual spaces to be searched, the data to be extracted, and its relation to the hypothesis of investigation.	Colombia is in line with Art. 19.5

Party	Legislative and other measures	Assessment
	- The evidence collected may be subject to exclusion in court for not complying with legal provisions, and/or affecting the privacy rights, Habeas Data, non-self-incrimination, and in general any other fundamental right. - The evidence may also be excluded on the grounds of violating professional secrecy and the protection of other liberal professions contained in the Constitution. - The extraction of information is limited to be carried out within no more than 30 days during the investigation phase and within no more than 15 days during the investigation phase or after the indictment. - The procedure carried out by the computer expert and the results obtained are subject to constitutional control by a Judge for the Control of Guarantees (Juez de Control de Garantías) within 36 hours after the completion of the activity. - During the legalization hearing and control of the procedure, it is possible for the defense to participate to oppose any of the phases exhausted for this purpose.	
Costa Rica	This measure applies to all investigations regardless of the type of crime. The authorities mentioned that there are no legislative developments regarding the means of obtaining digital evidence, such as a specific law, and so there are no safeguards regarding the search and seizure of digital data. Nevertheless, the general conditions of safeguards established in the Code of Criminal Procedure apply to the acquisition of any ordinary means of evidence. As a consequence of a lack of specific regulation on digital evidence, there are no safeguards specially designed for the measures provided for in art. 19. The general safeguards of criminal procedure apply by analogy.	Costa Rica is in line with Art. 19.5.
Croatia	Croatia applies judicial supervision and a number of other general conditions, limitations and safeguards to be respected prior, while and after the undertaking of a search (common provisions), which also apply to the Article 257. Articles 239, 242 and 243 of the CPC establish numerous safeguards for searches in general. These include (per Article 239) that the defendant must be informed of the grounds for being suspected, is not required	Croatia is in line with Article 19.5.

Party	Legislative and other measures	Assessment
	to answer questions or present a defence, has the right to see the evidence, and has a right to an interpreter and defence counsel. Article 64 of the CPC establishes an extensive list of defendant's rights with regard to all investigative measures. These rights include being promptly informed of the basis for the charge, having an interpreter if needed and defence counsel (paid by the government if necessary), and being able to examine the evidence, cross-examine witnesses, and remain silent. Articles 244 and 245 of the CPC permit certain rights of the defendant not to be applied in exceptional cases (as to Article 244 – non-deliverance of court warrant, bill of rights or request to hand over an object of search; as to Article 245 – substitution of the state attorney's warrant for a prior court warrant).	
Cyprus	Warrants can be issued for electronic search and seizure involving any crime. Cyprus requires the issuance of a search warrant/court order by a judge based on a police officer's written oath. The order must be necessary for the furtherance of the investigation and to avoid destruction of the evidence. Overall, it must be necessary and proportionate. Affected persons may challenge the warrant/order.	Cyprus is in line with Art. 19.5.
Czech Republic	Measures may be applied only in criminal proceedings also against other offences where evidence is on computer system, subject to reasonable suspicion that the computer system contains the evidence. House searches and search of other premises and places require court order. Orders to removal of items may be in limited circumstances issued also by the police authority. Court has to always assess the proportionality and necessity of such action (provision 2 par. 4 of the CPC). Court order has to include reasoning, it is served to the person at whom the search is executed. Person concerned has to be heard before the search, with exception of urgent cases, and he/she has right to be present during the search. The house search and personal search has to be executed in presence of the third person unrelated to the investigation and person concerned.	Czech Republic is in line with Art. 19.5.

Party	Legislative and other measures	Assessment
	The legislation also provides protection to individuals from being compelled to incriminate themselves, protection of legal privilege.	
Denmark	The regulations applicable to search and seizure contain numerous requirements, limitations, and protections. Beyond those already described, the requirements include notification, presence of the searched person or a substitute, attorney representation prior to the issuance of an order in some cases, the possibility of reversal of a court order, and, in general, a mandate that searches be carried out as gently as possible.	Denmark is in line with Article 19.5.
Dominican Republic	The Dominican Republic domestic legislation combines the same conditions and safeguards established in both the Dominican Constitution and the Code of Criminal Procedure, stipulating that searches may only be carried out at the request of the Public Prosecutor, with a search warrant issued by a reasoned judicial decision. In cases of urgency and the absence of the public prosecutor, the police may make a direct request. Law 53/07 does not expressly provide that the procedural rules included therein apply to the investigation of all crimes. Therefore, it is possible to interpret that the procedural powers of search and seizure of data would not be applicable to the investigation of all crimes, but only to the computer crimes provided for in this special law. Notwithstanding the above, Dominican Republic authorities reported that, in practice and jurisprudence, chapter II of Law 53-07 on procedural measures, including the powers contained in Article 54, are not linked to the offenses established by Law 53-07, and therefore are applicable to any offense with electronic evidence.	Dominican Republic is in line with Art. 19.5, however, it is advisable to amend the legislation to clarify that the procedural provisions apply to the investigation of all crimes.
Estonia	Measures of search and seizure apply to any offences and are limited to criminal investigations. As regards covert access which is considered as a surveillance activity, the law provides for a list or catalogue of serious crimes in which case the surveillance measures are permitted. Execution of powers is subject to judicial supervision. As a general rule, persons can challenge any procedural measure or act pursuant to the general rules on remedies. Both during the pre-trial investigation as well as trial face evidence obtained and procedural measures used are subject to the judicial review.	Estonia is in line with Art. 19.5.

Party	Legislative and other measures	Assessment
	Greater limitation is imposed with respect to the covert operations. With respect to notification, there are general rules concerning informing the person concerned about the measure concerned, rights and obligations as well as remedies.	
Fiji	The Fijian authorities reported that section 24 of the Fijian Constitution provides that the right to privacy should be considered. At the same time, Section 21 of the TCA provides for the safeguards further implementing section 24 of the Constitution. It lays down the rule and specifies the technical expertise needed to extract data whilst maintaining the privacy as enshrined in the Constitution. More specifically, Section 21 of the TCA provides safeguards for the process of searching and seizing stored computer data. The search request must meet certain requirements to protect the integrity and privacy of the data. It must state the reasons why the material sought is likely to be found in the specified computer system or storage medium. It must also specify the nature of the evidence that is likely to be found and the technical measures to be taken to carry out the search and seizure, giving priority to techniques such as mirroring or copying relevant data and avoiding, wherever possible, the physical custody of the computer system or storage medium.	Fiji is in line with Art. 19.5.
Finland	Section 21 of The CMA states the conditions for conducting a search of data contained in a device, requiring suspicion of an offense with a punishment of at least six months of imprisonment and the possibility of discovering relevant evidence. A search of data contained in a device and a remote search of data contained in a device may be conducted if the most severe punishment provided for the offence is imprisonment for at least six months. Technical surveillance of a device may be carried out if the most severe punishment provided for the offence is imprisonment for at least four years or if the offence is one of the offences listed in the provision. When applying the provisions on coercive measures in a specific case, the principle of proportionality must be considered. These measures may be used only if it can be considered justified, considering the seriousness of the offence under investigation, the importance of clarifying the offence, the extent to which the use of	Finland is in line with Art. 19.5.

Party	Legislative and other measures	Assessment
	the coercive measure violates the rights of the suspect of the offence or others, and the other circumstances. An official with the power of arrest decides on a search of data contained in a device and on a search of data contained in a device as a remote search. A police officer can make the decision in urgent situations. If a search may uncover information protected by the right or obligation not to testify in court, a court decides on the search and appoints a search representative. If, during a search, it becomes apparent that the search is aimed at the above-mentioned type of information, or if it is necessary to carry out the search urgently, an official with the power of arrest decides on the conduct of the search and on the appointment of the search representative. The court decides on technical surveillance of a device. If the matter does not brook delay, an official with the power to arrest may decide on surveillance until such time as the court has decided for the issuing the decision. If in a search something has been copied for the use as evidence, on the request of the person concerned in the matter, the court shall decide whether the copy of the document is to be retained to be used as evidence.	
France	The guarantees applicable to criminal matters, notably appellate rights, are equally applicable in these cases.	France is in line with Article 19.5.
Georgia	The powers are subject to safeguards, including mandatory judicial oversight, proportionality, grounds justifying application (probable cause), right to appeal, limitations, notifications, immunities, data protection requirements and right to remedies.	Georgia is in line with Art. 19.5
Germany	Measures are subject to requirements and safeguards in the national legal system. More specifically, every person concerned has a right to a fair trial, whereby the principles of the rule of law must be upheld. Other safeguards include necessity, proportionality, legality, judicial supervision and review.	Germany is in line with Art. 19.5.
Ghana	Article 18 of the constitution protects persons' privacy in their homes, property, correspondence or communications except in certain circumstances, in accordance with the law of a free and democratic society. Searches and seizures require warrants issued by a court except when carried out incident to an arrest or in limited other cases. Other potential protections include requirements for the chain of custody, photography	Ghana is in line with Article 19.5.

Party	Legislative and other measures	Assessment
	with markings, witnesses, making and retaining copies of relevant computer data and maintaining their integrity, and removing data from a searched system or rendering the data inaccessible only if the specific requirements of the law are met (see e.g. Sections 98 and 99 of ETA).	
Greece	Several principles "aim to strike a balance between the investigative needs of law enforcement and the protection of individual rights and privacy, ensuring that these measures are carried out lawfully and responsibly." The principles include compliance with legal authorisation, probable cause or reasonable grounds, protection of individual rights, data integrity and security, transparency and accountability, and preserving data in anticipation of trial.	Greece is in line with Article 19.5.
Grenada	Grenada authorities indicated that sections 26 to 32 of the Electronic Crimes Act provide for conditions for the seizure of stored data. The most important safeguards are judicial supervision, limited use of data and information. Other human rights safeguards are covered by the Constitution for all citizens and residents. Powers under Electronic Crimes Act apply to any offence as outlined in Section 22 (2) (c).	Grenada is in line with Art. 19.5.
Hungary	Section 2 of the CPC expressly protects human dignity and the right to liberty and security. Fundamental rights may be restricted only as specified in detail in Section 271 of the CPC and to the least possible extent. Seizures are to be terminated in the shortest possible time. The legal basis and manner of seizures of electronic data may be contested by affected parties. Complaints are forwarded to the prosecution for consideration.	Hungary is in line with Article 19.5.
Iceland	The powers for the search and seizure of stored computer data apply also to other offences under our domestic law where evidence is on a computer system. The most important conditions and safeguards applied in Iceland are judicial supervision, right of redress, proportionality, notifications, legal representation, limited duration of the measures.	Iceland is in line with Art. 19.5

Party	Legislative and other measures	Assessment
Israel	Searches and seizures of computer data may be conducted only relating to crimes with a maximum sentence of more than three months. Searches are governed by the State's Attorney Guideline and rulings in a Supreme Court case, CrimFH Urich, incorporated into the Police Guideline. Applications for computer search warrants must fulfil numerous specific requirements. Warrants must be issued by a judge and contain details of the purpose of the search and its constraints. The search must be necessary and the infringement on the privacy of the person affected must be limited.	Israel is partially in line with Art. 19.5, authorities should consider extending the scope of the measure to include all evidence where evidence is on a computer system
Italy	The powers for the search and seizure of stored computer data applies to any offence under domestic law. The conditions and safeguards are the same as those provided to the suspect by the Italian Criminal Procedure Code, namely: 1) presence of a defender (art. 356, 365), 2) drafting of a special report by the police (art. 357), and 3) the possibility to challenge the decree - after its execution - before a judge (art. 257).	Italy is in line with Art. 19.5.
Japan	Both the Constitution and the CPC declare safeguards and conditions. The Constitution states that all persons have the right to be secure in their homes, papers and effects and that warrants issued for adequate cause are required for searches and seizures. "Adequate cause" is defined and coercive measures not in the law are impermissible. Persons aggrieved by a search and seizure based on a warrant may file a complaint with the relevant court, bring a civil action, or seek compensation for damages based on another act.	Japan is in line with Article 19.5.
Kiribati	Section 29 of the Cybercrime Act provides safeguards when these intrusive procedural powers are utilised. Per that Act, the execution of powers under the Act is subject to conditions and eight safeguards pursuant to the Constitution and human rights obligations under applicable international conventions. In addition, proceedings for an offence under the Act may be commenced only with the consent of the Attorney General if the defendant was under 18 at the time he or she allegedly engaged in the conduct constituting the offence.	Kiribati is in line with Article 19.5.
Latvia	Article 219 that is applicable to extension of searches does not apply to all categories of search and seizure.	Latvia is partially in line with Article 19.5.

Party	Legislative and other measures	Assessment
	Searches can only be done after a decision by an investigating judge or a court or, at a minimum, with authorisation by a prosecutor in certain cases. Improperly-collected evidence is inadmissible at trial. Potential defendants have protections against self-incrimination that permit them to decline cooperation. Search and seizure powers are regulated by numerous statutory provisions.	Authorities should consider extending the scope of the measure to cover all offences where evidence is on a computer system
Liechtenstein	In general, court orders are required for searches and seizures. In practical terms, those measures are carried out by at least two officers, and all significant actions are discussed, approved and executed by at least two people. Those actions are then documented in a protocol with photos. The data analysis is always conducted using exact copies, not original data.	Liechtenstein is in line with Article 19.5.
Lithuania	Searches and seizures are governed and restricted by several articles of the CPC. Court orders authorising the measures are appealable by involved persons and by affected third parties.	Lithuania is in line with Article 19.5.
Luxembourg	In summary, any measures must meet the following standards: they must be approved by the Public Prosecutor or the investigating judge depending on the circumstances, be duly substantiated, not go beyond what is necessary to establish the truth and be limited in time. The person concerned must be notified of the measure within a certain period and can be present during the search. All unnecessary data must be deleted. Luxembourg listed numerous statutory provisions that include specific elements that are protective of human rights.	Luxembourg is in line with Art. 19.5.
Malta	Pursuant to Chapter 9 Article 355I of the Criminal Code – *'The executing officer shall hand over a copy of the warrant to the person occupying and present at the place searched or to any other person who appears to the said officer to be in charge of the same place and who happens to be present during the search. If there is no person present who appears to the executing officer to be in charge of the premises the copy of the warrant shall be left in an easily visible place on the premises.'* Pursuant to Chapter 9 Article 355J of the Criminal Code – *'A search under a warrant may only be a search to the extent required for the purpose for which the warrant was issued.'*	Malta is in line with Article 19.5.

Party	Legislative and other measures	Assessment
	Seized equipment is stored securely. Devices to be analysed by experts are released promptly by the police to that expert or they are retrieved from secure storage by police analysts prior to the start of the analysis. The police lab can be accessed only by the Digital Forensics team and a CCTV system provides further security.	
Mauritius	The application of Section 28 is subject to judicial control. In addition, an accused's right to a fair trial is protected under the Constitution. Applications for searches and seizures are normally made ex parte, but, if a judge is not satisfied by the application, the judge may have the interested party appear in court if there is a serious risk of violation of human rights or the rights to privacy or property. If an order has already been issued, a sufficient showing by the interested party may cause the judge to set aside the order. Mauritius stated that, although the Act lists offences in its Part III, the use of Section 28's investigative powers is not restricted to those offences. Section 14 of the old Computer Misuse and Cybercrime Act 2003 (now repealed) was couched in words similar to the present Section 28 of the Cybersecurity and Cybercrime Act. Repealed Section 14 provided for access, search and seizure "for the purposes of an investigation or the prosecution of an offence." In Lee Wai Chung & Anor v The Independent Commission Against Corruption [2021 SCJ 37], an order was granted under Section 14 for the access, search and seizure of electronic data. Apparently, the offence being investigated was an offence under the Prevention of Corruption Act, not the CMCA. The granting of this order supports the point that present Section 28 of the CCA and repealed Section 14 of the CMCA were broadly drafted to encompass any offence. Thus, the scope of application of Section 28 is not limited to offences under the CCA. In addition, the Financial Crimes Commission, set up under the newly enacted Financial Crimes Commission Act, is mandated, by virtue of section 60 of that Act, to enter and search any premises and collect evidence in electronic form for "an investigation."	Mauritius is in line with Article 19.5.

Party	Legislative and other measures	Assessment
	Finally, there are cases (Police v Chady & Maunthrooa [2019 INT 228]) where "electronic evidence" was collected and was admissible before the Court for a corruption offence. This case also supports the point that investigative powers may be used in relation to other statutory offences.	
Monaco	Seizures and examinations of data must be ordered or ratified by a judicial authority (of different types, depending on the investigation). Evidence may be suppressed if the law was violated during the investigation or its evidentiary reliability may be questioned if it was not protected from manipulation. Targets may request additional investigation or expert views. Data may be seized by sealing the physical medium or by making a secure copy in the presence of the person concerned.	Monaco is in line with Art. 19.5.
Montenegro	Constitution of Montenegro and the Criminal Procedure Code provide general conditions and safeguards which secure adequate protection of human rights and liberties. The measures are applied in relation to investigation of criminal offences. Execution of powers is subject to judicial supervision.	Montenegro is in line with Art. 19.5.
Morocco	Every investigation is supervised by the Public Prosecutor, and searches and seizures make take place only with the authorisation of the Public Prosecutor or the investigative Judge. The proceedings must take place in the presence of, and with the explicit consent of, the affected person. Numerous other conditions and prerequisites apply as laid out with specificity in Articles 103 through 116 of the CPC.	Morocco is in line with Article 19.5.
Netherlands	Powers granted by law for the search and seizure of stored computer data apply to all offences under domestic law where evidence is on a computer system. For all procedural powers the law requires respect for human rights, enshrined in the constitution of the Netherlands, the Charter of Fundamental Rights of the EU, ECHR, or in other treaties to which the Netherlands is a party. The procedural powers are written down in the DCCP (legality). In most cases, they require explicit consideration of proportionality and subsidiarity. Execution of powers is subject to judicial supervision and/or decision.	Netherlands is in line with Art. 19.5.
Nigeria	The Nigerian Constitution provides for safeguards when dealing with the property and data privacy of its citizens. See sections 144 of CFRN and 37 respectively.	Nigeria is in line with Article 19.5.

Party	Legislative and other measures	Assessment
	The Administration of Criminal Justice Act makes provisions regarding the process and procedure during a search and seizure. See sections 143-153 and 333-338 respectively. These processes and procedures preserve the rights of citizens. The procedure for searches and seizures under Nigerian laws, including the Cybercrimes Act, takes the utmost account of fundamental human rights and constitutional safeguards. Hence, save for cases involving minors, no formal process(es) can be dispensed with. A judge making an order pursuant to section 45 must be satisfied that all formal processes have been followed, including having "reasonable grounds to believe." See section 45(3)(c) of the Cybercrimes Act. Nigerian laws provide for arrest without warrant. However, in the case of searches and seizures, an officer may not act without a warrant, except in limited circumstances; e.g. where a minor is involved This is to preserve fundamental human rights of citizens. Section 45 of the Cybercrimes Act provides for the issuance of a warrant by a judicial authority when an investigation relates to specified offences or under certain circumstances. Generally, beyond section 45, some safeguards during a search and seizure may include: - Right to be informed of the alleged offence. - Right to be shown a copy of the search warrant. - Right to remain silent. - Presumption of innocence. - Right to be present and have witnesses during a search. - Right to have an inventory of all items seized during a search. - Right of a woman not to be searched by a man, etc.	
North Macedonia	According to CPC Articles 181.2., 186.2., 189, 190.1, 190.3. and 191, a court will issue an order pursuant to the prosecutor's request, which must contain an explanation/justification. The order will be aimed at a precisely defined data carrier or sub-flow or transfer of data, especially when the system involved serves multiple users or systems. The order may also take into account matters of data protection and the efficient transfer of data. Searches are performed only on the parts of a system that are relevant to the specific criminal case.	North Macedonia is in line with Article 19.5.

Party	Legislative and other measures	Assessment
Norway	The CPC contains a provision requiring proportionality when coercive measures are used. Other sections address the duty of confidentiality and protection of the right against self-incrimination. The European Convention on Human Rights applies in Norway and is applied by Norwegian courts.	Norway is in line with Article 19.5.
Panama	Powers granted by law for the search and seizure of stored computer data are used for offences against computer systems or computers, as well as in relation to other offences under national legislation. There are no safeguards expressly provided for such measures. What should be considered is that, for the data obtained from searches or extended searches to be valid in the process or trial stage, due process must be complied with the right to a defense, and that the Prosecutor must comply with the respective constitutional controls of guarantees, before the Judge, whether prior or subsequent. There are no safeguards expressly provided for such measures. What should be considered is that the Panamanian criminal procedure establishes a series of controls precisely to ensure respect for Human Rights and the Individual Rights and Guarantees that every person has. For data seizure, for example, the regulation provides for subsequent oversight by a Judge of Guarantees. In such cases, the Prosecutor carries out a seizure of data stored. in a computer system and must submit their actions to the Judge within a period of ten days. The Judge will verify 1. That the defense has been notified of the proceedings, ensuring the right to defense. 2. The existence of a criminal investigation that justifies the actions taken by the Prosecutor (due process). If the data involve correspondence or private information, the procedure is different. In strict adherence to the inviolability of correspondence, such a measure must be justified. Before a judge in advance, except for specific circumstances established by the law, which must be subsequently justified.	Panama is in line with Art. 19.5
Paraguay	The provisions on search and seizure of data apply to the investigation of any crime. The conditions and safeguards to apply in the records is that the warrants must describe the electronic devices or other objects to be seized, and the conditions to be considered is that only the things that were authorised should be seized.	Paraguay is in line with Art. 19.5

Party	Legislative and other measures	Assessment
	Regarding the extension and seizure of computer data, only the data in the time frame of the events can be seized, also only the data of users involved, and the data of events linked to the reported crimes. In another response to the questionnaire, the report quotes an important provision of the constitution that reaffirms constitutional guarantees, namely Article 36 on the Right to the Inviolability of the Documental Patrimony and of the Private Communication.	
Peru	The measures under restricting rights that is regulated in article 217 of the Criminal Procedure Code is applicable to crimes against or through computers and to other crimes typified in domestic law when the evidence is found in a system computer. Safeguards refer to what has been answered throughout the entire report, does not specifically address to digital evidence.	Peru is in line with art. 19.5.
Philippines	A court issues warrants for searching, seizing and examining data. That court involvement "ensures the balance between the right of the government to conduct criminal investigations and the citizens' right to privacy and freedom from unreasonable searches."	The Philippines is in line with Article 19.5.
Poland	The conditions and safeguards in the CPC that are applicable to the general rules of search and seizure are also applicable in the electronic world. These provisions guarantee the protection of human rights and freedoms. Numerous articles in the CPC are relevant (see Poland's detailed submission). Overarching protections include that an accused shall be presumed innocent until guilt is recognised in a judgment that is final and that an accused has the right to defence counsel and must be advised of this right. More-specific protections include requirements for the presence of the person concerned in a search or a suitable substitute. Among other requirements, searches or seizures of objects must be conducted "with moderation and within the limits necessary" to achieve the objective with due respect for the privacy and dignity of the relevant persons.	Poland is in line with Article 19.5.
Portugal	Other than in the limited circumstances described, searches and seizures must be authorised by a prosecutor or judge. The measures are subject to the restrictions in the Cybercrime Law. Searches must be notified to the concerned person or a proper substitute. If particularly private data are seized, the data must be submitted to a judge, who will consider whether it is necessary to the case. Special protections apply to the	Portugal is in line with Article 19.5.

Party	Legislative and other measures	Assessment
	data used in certain professions, such as medicine or journalism. Search and seizure orders must be executed within 30 days, and seized data must be retuned as soon as it becomes unnecessary as evidence.	
Republic of Moldova	Moldova cites five statutes (CPC Articles 11 – 15, covering inviolability of the person, home, correspondence (including telephone conversations) and property; procedures for searches and seizures). These articles bar measures such as search and seizure except when they are conducted pursuant to the CPC. The CPC requires pre-action warrants, post facto court ratification of actions taken without warrants, seizures of property only pursuant to a court decision and with minutes of the proceedings, and other detailed restraints on, and requirements for, searches and seizures.	Moldova is in line with Article 19.5.
Romania	Searches and seizures that are considered "necessary" are normally authorised by a court based on an application that must supply numerous details. Copies are made to ensure the integrity of the evidence and detailed reports and documentation of the search are required. The search is conducted without unjustifiably making public aspects of the private life of the targeted person. Searched data that are of a secret nature is protected.	Romania is in line with Art. 19.5
San Marino	San Marino stated that the measures are subject to conditions and safeguards of its domestic law. More specifically, various principles of their domestic legal framework (proportionality, appropriateness) and constitutional rights (privacy) of individuals are applicable. However, they indicated that, in the implementation of seizures, keywords should be used to search for relevant data on seized devices.	San Marino is in line with Art. 19.5.
Senegal	As noted above, per CPC Articles 90-4 through 90-6 and 90-8, searches are authorised and supervised by the Prosecutor of the Republic or by a juge d'instruction. They are executed by the juge d'instruction or by the judicial police under the supervision of the prosecutor or juge d'instruction. Searches are permissible only if the targeted data are absolutely necessary to the investigation, with strict conformance to the principle of the legality of evidence. The data must be useful for the purpose of determining the truth. The person in charge of the system must be informed about the search carried out and about the data copied, removed or rendered inaccessible.	Senegal is in line with Article 19.5.

Party	Legislative and other measures	Assessment
	The use of lawfully acquired credentials and of technical processes, programs, etc, to restore deleted data or for attribution is permitted only when necessary to obtain evidence and must be authorised and supervised by the prosecutor or juge d'instruction. Subject to applicable international arrangements, a judge may collect stored data in a system other than the initial system located in another place on or outside Senegalese territory, assuming that the subsequent system is accessible from the initial system. Such extension must be necessary to determining the truth or there must be risks of loss of evidence without the extension. The extension must reach only those systems to which persons authorised to use the initial system have access. The judge must inform the person in charge of the system unless their identity or address cannot be found. Articles 90-1 to 90-14 of the CPC provide for the copying, maintenance and preservation of the integrity of seized data. Persons with possession or control of data may be required to protect its integrity. In addition to the human rights protections in the laws of Senegal, Law No. 2008-12 protects personal data.	
Serbia	The conditions and safeguards in the CPC apply to all the elements of Article 19. In addition, the Law on Protection of Personal Data, the Law on Electronic Communications (to the extent that electronic data has personal implications) and other related laws and bylaws are all applicable.	Serbia is in line with Article 19.5.
Sierra Leone	The authorities reported that the enforcement officer shall apply to a High Court Judge stating the reasons for application of a warrant to search and seize and the Judge may or may not grant the application. This is under section 10(1-4). This safeguard is to ensure fairness and prevent abuse of powers. Also, section 10(8) makes provision for punishment for a law enforcement officer or any other authorized person who intentionally, recklessly, or negligently misuses their powers granted under section 10. This may include a fine or imprisonment. Proportionality of the measures is reflected for instance in Section 10(7). More specifically, an enforcement officer shall only seize a computer system if it is not practical to secure the computer data or necessary to	Sierra Leone is in line with Art. 19.5.

Party	Legislative and other measures	Assessment
	ensure that data will not be destroyed, altered, or interfered with or to exercise reasonable care while the system or computer data storage medium is retained according to section 10 (7a-b). Additionally, the enforcement officer should make a list of what has been seized or rendered inaccessible, with the date and time of seizure, and give a copy of that list to the occupier of the premises or the person in control of the computer system.	
Slovak Republic	The principles of proportionality, necessity and respect for fundamental rights, as regulated by the Constitution, the European Court of Human Rights, and the European Union Charter, are followed with regard to search and seizure. These measures are established under the CPC and warrants that meet the requirements must be obtained.	Slovak Republic is in line with Art. 19.5.
Slovenia	The CPC closely regulates searches and seizures and establishes numerous requirements, including the following. Warrant applications must meet several specified standards. Searches are sometimes done by consent, for which other requirements must be satisfied. When searches are done by order, a copy of the order must be provided to the interested person before the search. Electronic investigations of attorneys' data require a court order. The application and order must identity the items to be searched and must provide the justification for the search and other important details. Persons in certain categories – the owner of a device, for example, or the owner's attorney – have the right to be present. Investigations must prejudice the rights of third parties to the smallest possible extent, protect the confidentiality of data, and, in general, not cause disproportionate damage. Detailed documentation of the search is created, and evidence may be inadmissible if improperly obtained.	Slovenia is in line with Article 19.5.
Spain	Measures can be used/applied in any criminal investigation — crimes committed in computer systems or crimes committed in a physical environment — provided that the assumptions justifying such an intervention in accordance with proportionality criteria are met. Article 18 of the Spanish Constitution guarantees the protection of the fundamental rights to privacy, the inviolability of the home; the secrecy of communications and the protection of personal data in such a way that any investigative measure involving interference with any of these rights requires the consent of the data subject or express and reasoned judicial authorisation.	Spain is in line with Art. 19.5

Party	Legislative and other measures	Assessment
	Spain has been referred to the requirements established by the Budapest convention to safeguard the rights of individuals during investigations. Among these requirements are the mandatory intervention of the judicial authority, the reasoned resolution that assesses the principles of specialty, necessity, suitability, exceptionality and proportionality, the delimitation of the content and scope of the search, the separate authorisation of prolonged searches and the decision of the judicial authority on the measures necessary to guarantee the authenticity and integrity of the data. In addition, they mentioned Chapter IV of Title VIII of Book II of the Spanish Criminal Procedure Act regulates general provisions applicable to all technological investigative measures, such as the permanent control of the investigation by a judicial authority and specific rules for using the information in different judicial proceedings.	
Sri Lanka	Sections 20, 22 and 24 of the Computer Crime Act set out conditions to be met when searches and seizures take place. They make provision for avoiding disruption of businesses if possible, inventorying and perhaps providing copies of seized items, and preserving the confidentiality of the proceedings.	Sri Lanka is in line with Article 19.5.
Sweden	Specific requirements relating to search and seizure are described above. Beyond these requirements, overarching human rights principles apply to coercive measures (including search and seizure). These principles include proportionality, which is explicitly mentioned in the relevant legislation; legality; purpose; and need. The Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms is directly applicable as law in Sweden. In general, coercive measures may be challenged in court by the affected person. The authorisation and execution of secret surveillance, including secret data interception, are regulated by specific laws and regulations, including the Secret Data Interception Act. Authorisations for secret data interception must normally be ordered by a court. The Commission on Security and Integrity Protection supervises the use of secret surveillance, including secret data interception, by law enforcement. This supervision particularly attempts to ensure that such activities are conducted in accordance with laws and other regulations. The supervision is exercised through inspections and other investigations. The Commission may make statements about the facts it establishes and express its opinion about the need for changes to practices; in addition, it "shall strive to ensure that	Sweden is in line with Article 19.5.

Party	Legislative and other measures	Assessment
	any deficiencies in laws and other regulations are remedied." On the request of a person, the Commission must determine whether they have been the subject of secret surveillance and whether its use and associated activities were in accordance with laws and other regulations. The Commission must notify the person that the examination has been carried out.	
Switzerland	Under the CrimPC, certain elements are prerequisites for coercive criminal procedural measures. Such measures may be taken only if they are permitted by law and if there is sufficient suspicion of a crime. In addition, such measures must be necessary and reasonable. An aggrieved person may object to rulings and to the procedural acts of the police, prosecutor and other authorities, and the rulings may be appealed. There are also specific safeguards, such as for the sealing of evidence and certain prohibitions on seizures.	Switzerland is in line with Article 19.5.
Tonga	Tongan safeguards derive from search and seizure practice in general and also from practices specific to data searches. First, measures established by Section 9 of the Computer Crimes Act are permitted only after issuance of a warrant based on an officer's affidavit that fulfils numerous statutory elements. There are provisions for the protection of the seized evidence (including for defendant's benefit). The normal safeguards in the Tonga Police Act also apply to data searches. Second, Tongan practices involve forensic experts at various stages, including pre-search. The specific powers in the Computer Crimes Act relating to search and seizure apply only to offences against or by means of computers. The more-general search and seizure powers under other acts, however, may be utilised in investigating any offence. Provisions for search and seizure under Magistrate Courts Act and Tonga Police Act can be applied generally to any offence but the wording and specifics of the warrant are critical to cover all aspects of evidence including digital and physical evidence.	Tonga is in line with Article 19.5. Authorities could consider extending the scope of the CCA to cover explicitly all offences where evidence is on a computer system.
Tunisia		
Türkiye	Searches and seizures are regulated by statutory or Bylaw provisions. The prosecutor is responsible for preventing searching officers from exceeding their duties and must give the necessary orders and instruction. Prosecutors must also obtain court warrants for searches or ratifications of executed searches. A suspect may appeal a judge's decision at any time, and that appeal is itself appealable.	Türkiye is in line with Article 19.5.

Party	Legislative and other measures	Assessment
Ukraine	Criminal proceedings must be carried out in accordance with the procedure and principles clearly defined by law, in relation to persons involved in criminal procedural activities, in order to achieve the effectiveness of criminal proceedings (to prevent and terminate illegal actions, ensuring the detection and consolidation of evidence, etc.). Temporary access to things and documents consists in providing a party to criminal proceedings by a person in possession of such things and documents with the opportunity to get acquainted with them, make copies of them and seize them (seize them). Temporary access to electronic information systems or their parts, mobile terminals of communication systems shall be carried out by making a copy of the information contained in such electronic information systems or their parts, mobile terminals of communication systems, without removing them.	Ukraine is in line with Art. 19.5.
United Kingdom	The UK authorities reported that all UK legislation relating to the investigation of criminal offenses meets international standards for the protection of individuals. In the case of PACE, a warrant can only be applied for if it meets the criteria set out in the Act and Code of Practice B, and the decision is taken by a court rather than the police. PACE Code B provides that the right to privacy and respect for personal possessions are fundamental principles of the Human Rights Act 1998. Powers of entry, search, and seizure should be fully and justified before use because they may significantly interfere with the occupier's privacy. Powers of search and seizure must be used fairly, responsibly, with respect to the people who occupy the premises being searched or are responsible for the property being seized, and without unlawful discrimination. In addition, in Scotland, only targeted, proportionate examinations of digital devices (to extract data) should be carried out and only where necessary to pursue a reasonable line of inquiry. Examination of digital devices will not be carried out routinely, and before ordering such examination, prosecutors should be satisfied that it is strictly necessary. Where a warrant is issued in Scotland, it can only be issued by a Justice of the Peace	United Kingdom is in line with Article 19.5.

Party	Legislative and other measures	Assessment
	or a Sheriff. They must have the appropriate expertise to carry out this role and must also act in a manner consistent with the ECHR when deciding whether to grant the warrant.	
United States	Applicable protections and safeguards include the provisions of the Constitution, particularly those relating to searches and seizures and to self-incrimination. Search warrants are issued only by an independent judge and applications for warrants must meet high standards. The Federal Rules of Criminal Procedure and some statutes limit the scope of warrants by, for example, restricting the period for execution of a warrant. Evidence obtained in violation of the protections and procedures may be inadmissible at trial.	The United States is in line with Article 19.5.

9 CONCLUSIONS AND RECOMMENDATIONS

As indicated at the outset of this report, Article 19 is an important procedural power under the Convention. Sharing of information and experience on practices and legislative and other measures in implementing Article 19 will facilitate further reforms in current and future Parties where necessary. Furthermore, the question of the extension of searches to other Parties' territories, which is linked to the domestic procedure of Article 19.2, continues to be of interest of the T-CY, since several Parties have in place national provisions that allow authorities to conduct that type of procedural measures. The T-CY, therefore, carried out a detailed assessment of the implementation of Article 19 in the domestic law of the Parties to the Convention.

The assessment was based on replies from [74] Parties. Discussions were held at the 28th Plenary (June 2023), 29th Plenary (December 2023), 30th Plenary (18-20 June 2024) [and 31st Plenary (11-12 December 2024) which also adopted the present report. In line with obligations under the T-CY Rules of Procedure, all responding Parties submitted rich and detailed responses to the questionnaire. Most of them also promptly provided any necessary clarifications. However, the assessment process and meeting agreed timelines set by the T-CY faced certain difficulties due to delays in the submission of initial responses and subsequent clarifications by some Parties.

The T-CY:

- considers that the assessment of the implementation of Article 19 of the Convention will enhance the effectiveness of this treaty;
- welcomes the replies to the T-CY questionnaire received from 74 Parties and the additional clarifications provided by most of these Parties;
- regrets that only partial replies were received from Tunisia and that, as a result, Tunisia could not be assessed;
- calls on all Parties to participate actively and in a timely manner in future assessments in the interest of the effectiveness of the Convention and the functioning of the T-CY;

9.1 Conclusions

9.1.1 Overall conclusions

Concl 1 **Specificity of procedural power in domestic statutory legislation** – Some of the Parties that implemented Article 19 largely rely on general powers (such as traditional search warrant powers, for example, to search a house or seize a tangible object) to meet some or all of the requirements of Article 19. Other Parties use specific powers that may target computer systems or computer data. The T-CY strongly encourages that powers, whether general or specific in nature, are sufficiently detailed to ensure that electronic evidence can be effectively collected and utilised in law enforcement investigations and prosecutions. Laws that rely solely on provisions relating to the search and seizure of tangible "objects" may not always cover all scenarios.[68] Article 19 is most effective when these general fundamentals are supplemented by statutory text or other measures that are specific to the digital

[68] It should also be noted that different rules may apply if powers of search and seizure of stored computer data are carried out in the location where the computer system or data are found, in another location (for example in computer forensic laboratories) after the initial seizure of the computer system or from another location in the case of an extension of searches.

world. Appropriate specificity can also be important for the adequate implementation of the conditions and safeguards of Article 15 (see corresponding recommendation 1).

Concl 2 **Legal jurisprudence and law enforcement practice** – Many Parties stated that the procedural powers of Article 19 have been applied in criminal investigations or proceedings by considering general principles of evidence law, such as the "principle of freedom of evidence" mentioned by some Parties in their responses to the questionnaire. Others noted that such principles were shaped by case law or supplemented by domestic customary procedural practice and law enforcement manuals to inform law enforcement practice.

However, the execution of procedural powers for search and seizure of stored computer data has become more complex with new technological challenges (such as the growth of data storage, encryption, cloud hosting, etc.). The search and seizure of virtual assets to be used as evidence was mentioned by some Parties as one of those technological challenges.

All of these challenges make it increasingly difficult to rely on jurisprudential interpretation, guidelines or accepted practices to resolve perceived gaps in statutory frameworks or other forms of domestic law established originally for physical evidence. It is therefore increasingly advisable for countries to adopt statutory measures to implement Article 19 of the Budapest Convention instead of leaving the application to case law, best practice or manuals alone. This may also enhance compliance with Article 15 and ensure legal certainty for both law enforcement and those accused of crimes (see corresponding recommendation 1).

Concl 3 **Core definitions of the Budapest Convention** – Some Parties have not implemented the definition of computer data in Article 1 of the Convention in their domestic law. While the Budapest Convention does not oblige Parties to copy into their domestic laws ad verbatim the four concepts in Article 1 of the Budapest Convention[69], it is critical that statutory measures (such as domestic legislation) cover such concepts to confidently ensure that procedural powers can effectively seize electronic evidence, that is, computer data (see corresponding recommendation 2).

Concl 4 **Emails stored by the service provider and unopened by the recipient** – Some Parties treat an unopened e-mail message waiting in the mailbox of a service provider until the addressee downloads it to their computer system as stored computer data to which Article 19 applies. Other Parties treat it as data in transmission whose content can only be obtained by applying the power of interception. Others did not specify. While such questions may be addressed in guidance documents adopted at the national level, not all Parties have adopted such guides (see corresponding recommendation 3).

Concl 5 **Value of continuous training and guidance** – A number of Parties indicated that their competent authorities rarely or never make use of certain search and seizure powers (even in cases where the measures are provided in the domestic law). Lack of practical experience or the availability of training to gain the necessary knowledge may play a role in this. Sustainable training and guidance appear to be an important element to acquire the necessary skills and to ensure that the measures are used appropriately and under conditions and safeguards (see corresponding recommendation 4).

[69] See paragraph 22 of the Explanatory Report to the Budapest Convention.

Concl 6 **Value of capacity building** – A considerable number of Parties have adopted legal provisions in line with Article 19 following support by the capacity building projects of the Cybercrime Programme Office of the Council of Europe (C-PROC) and, furthermore, have received training and other assistance to apply these provisions. Such support will also be available in the follow up to the conclusions and recommendations of the present assessment report (see corresponding recommendation 18).

9.1.2 Conclusion on the implementation of Art. 19.2

Concl 7 **Extension of a search or similar accessing in the territory of a Party to a computer system or part within the territory of that Party** – Generally, Parties are able to extend their search or similar access to another computer system or part of it in their territory as required by Article 19.2.[70] Although some countries do not expressly provide for such a situation in their legislation, they have either applied this during investigations without encountering concerns or have accepted it through case law decisions (see corresponding recommendation 5).

9.1.3 Conclusions on the implementation of Art. 19.3

Concl 8 **Copying stored computer data during search and seizure** – Many Parties noted that they have the power to copy computer data. Parties, however, have different understandings in the exercise of this power. Some Parties use the power only after the seizure of a computer system in order to preserve the integrity of the data. While this is an important aspect, the power of copying should also cover situations of on-the-spot copying, as in some cases copying may be preferable to seizure. This may, for example, cover situations that require minimising harm to an individual when the rights, responsibilities and legitimate interests of third parties may be at stake. On-the-spot copying may also assist in reducing risks of inadvertent or intentional deletion of electronic evidence that may occur before a seized computer system can be forensically analysed. Selective copying during a search may also reduce the volume of data that forensic specialists must analyse (see corresponding recommendation 6).

Concl 9 **Maintaining the integrity of stored computer data during and after seizure** – Most Parties had difficulties explaining the source of their power to maintain the integrity of the data. Such requirement may perhaps be addressed in secondary legislation and guidance documents (see corresponding recommendation 7).

Concl 10 **Removal or rendering stored computer data inaccessible** – Most Parties did not clearly have the powers to remove data from a searched system or to render them inaccessible (subject to human rights safeguards). This measure also does not appear to be used very often in practice.[71] Such powers are to address situations where the authorities have access to the data[72] and the circumstances of the case may require immediate deletion of the data or rendering them inaccessible by those authorities

[70] For example, law enforcement from a Party finds a computer during a house search and accesses a browser-based email account that contains emails stored remotely on the email services' server that is also located in the territory of that Party.

[71] The power covers only situations when the data are accessed by authorities. It does not cover removing online data or rendering them inaccessible through notice and take-down or other means to make a website unreachable by ordering third persons (e.g. service providers) to carry out the measure.

[72] Data may be stored on a computer system, on a computer data-storage medium or remotely accessible from the computer system being searched (for example data that is hosted in the cloud and accessed from the device seized).

to prevent the continued criminal use of data or the continued victimisation of victims. For example, these situations may involve danger or social harm, such as malware. Furthermore, there is an increasing need for removal of illegal content (for example, child sexual exploitation and abuse materials or intimate images distributed non-consensually)[73] (see corresponding recommendation 8).

9.1.4 Conclusion on implementation of Art. 19.4

Concl 11 **Compelling third party assistance in accessing computer systems or stored computer data** – Parties gave a wide range of responses about their ability to compel any person with knowledge of the functioning of a computer system, or measures applied to protect its data, to provide, as is reasonable, the information necessary to carry out the actions under Article 19.4. The power to compel assistance may be crucial to an accurate and complete search for evidence. Yet some Parties did not seem to have fully implemented this aspect of Article 19.[74] Frequently, a country could compel only one or two categories of persons; statutes might assume that searches would always be done only at business offices, so the assistance of people such as friends or roommates could not be compelled; often countries tried to apply an older statute to this clearly-digital measure.[75]

As noted in the Explanatory Report to the Convention, this power is not only of benefit to the investigating authorities. Without such cooperation, investigative authorities could remain on the searched premises and prevent access to the computer system for long periods of time while undertaking the search. In the absence of this power, the rights and obligations of third parties, including service providers and their customers, could be adversely affected. Limits on which third parties can be compelled to assist in computer searches, may result in Parties resorting to more intrusive measures such as seizure of the whole computer system or interception of content data if the Parties could not compel a person with the knowledge about a computer system to provide the necessary information.

Reasonable implementation of this power may thus help authorities to better incorporate the principle of proportionality. For example, providing the necessary information to enable the undertaking of the measures can help authorities to obtain the necessary data through copying, which is a less intrusive measure than seizure of the whole computer system or interception of content data. Full implementation of Article 19.4 thus constitutes an important safeguard, provided that it is applied in accordance with the principle of proportionality (see corresponding recommendations 9 and 10).

9.1.5 Conclusions on implementation of Art. 19.5

Concl 12 **Scope of the powers** (**value of electronic evidence collection for all crimes)** – A few Parties have powers to search and seize computer data pursuant only to a limited statute or only in cases that involve computer crimes. Other countries rely on a combination of statutes. Occasionally, the complex interplay of these statutes seems to mean that the powers to search and seize stored computer data apply only

[73] The lack of implementation of Article 19.3.d of the Budapest Convention in domestic law could lead to a situation where the authorities return a searched computer system to the offender that may still contain illegal content.

[74] Some Parties normally excluded targets or defendants from the requirement to assist with a search. This exception to the "any person" rule in Article 19/4 is permissible because Article 19 is subject to human rights safeguards, including the fundamental rights of defendants.

[75] The right against self-incrimination applies in some Parties, while others consider that the execution of such a measure is not subject to this right.

to certain categories of criminal offences. At the moment, in some countries, it may be possible to work around these gaps in the powers to search and seize. For example, the authorities may mainly use the powers for computer intrusion, electronic fraud, and closely-related cases. But the irreversible trend is that computer data will be relevant in all types of cases, including offline crimes that may involve electronic evidence (see corresponding recommendation 11).

Concl 13 **Safeguards and conditions applying to Article 19** – All Parties replied that the establishment, implementation, and application of powers under Article 19 are subject to conditions and safeguards provided for under their domestic law. As the Convention applies to Parties of many different legal systems and cultures, the reported conditions and safeguards not surprisingly differ between the Parties. Furthermore, Parties took different approaches to addressing the safeguards in their responses to the questionnaire: some responded with broad discussions of fundamental national documents, while others confined their answers to defendants' specific rights during investigations and at trial. Further work to identify how the Parties implement certain elements of Article 15 of the Convention (such as, for example, the right against self-incrimination, the question of privileges and immunities, etc.) may be of interest to the Parties to the Convention (see corresponding recommendation 12).

Concl 14 **Applications for and content of a search and seizure order** – Parties provided various responses regarding the content of an order that authorises a search. It can be inferred from responses of some of the Parties relying on implementation of Article 19 through general powers, that generic authorisation of a house search includes the search of a computer system or computer data even when an electronic search is not mentioned. Other Parties require a more specific approach, that is, an order specifying that a computer system or computer data identified during the execution of the search can be searched. The latter approach may provide a stronger case that a specific domestic procedural power can facilitate the conditions and safeguards required under Article 15, including the principle of proportionality (see corresponding recommendation 12).

Concl 15 **Application of privileges and immunities to computer data searched and seized** – Some Parties pointed out that computer data obtained may be protected by certain privileges and immunities from serving as evidence at trial (lawyer-client communication, physician-patient privilege, protection of journalistic sources, etc.). This is in line with the requirements of the Convention framework[76] (see corresponding recommendation 12).

Concl 16 **Impact of search and seizure procedural powers on third parties** – To the extent consistent with the public interest, the Convention requires that its Parties consider the impact of the powers and procedures upon the rights, responsibilities and legitimate interests of third parties.[77] Several Parties emphasised that measures of search and seizure are applicable only when the harm to the rights and interests affected is not greater than the benefit that their use provides for the public interest and third parties (see corresponding recommendation 12).

9.1.6 Other relevant conclusions

The following conclusions relate to issues that arise frequently in connection with Article 19 searches and seizures but are not addressed by the article. Parties provided extensive

[76] See para 147 of the ER to the Budapest Convention.

[77] See Art. 15.3. of the Budapest Convention.

information about these related issues, thus it seemed important to compile that information and make it available:

Concl 17 **Search and seizure procedure during emergencies** – Parties shared information about how they handle emergencies or other urgent situations in which a search or seizure may be necessary. Some Parties had no views about what situations would warrant an "emergency" search, while others defined "emergency" broadly, beyond physical emergencies. For others, the risk of destruction of evidence would merit an emergency search. In short, some Parties had no special mechanism for reacting quickly, while others could conduct emergency searches in a broad range of circumstances (see corresponding recommendation 13).

Concl 18 **Use of lawfully acquired credentials** – Many Parties have empowered their authorities by domestic law to use lawfully acquired credentials as part of a search (such as using login details for a computer system). However, responses of some other Parties indicate that the use of lawfully acquired credentials is not regulated. Some Parties also provide for the ability for law enforcement to seek a court order to compel or facilitate a person to provide such credentials to law enforcement to support a search (see corresponding recommendation 10).

Concl 19 **Covert remote accessing of computer systems through lawful computer exploitation activities** – The assessment demonstrated differing understandings by Parties of the measure of covert remote search of a computer system. There is a group of Parties that have adopted specific powers that enable the use of computer exploitation practices (such as the use of specialised software) to lawfully search a computer system remotely. Other Parties implement the measure through general powers (surveillance of persons, undercover investigations) or other measures that resemble implementation of Article 21 of the Convention. Some Parties do not provide for such a measure in their domestic laws (see corresponding recommendation 15).

Concl 20 **Extension of a search from the territory of a Party to computer data known to be outside the territory of that Party** – As regards the extension of searches to data known to be or reasonably suspected to be outside a State's territory, there are significant differences in approaches. The Convention does not address such extensions. However, due to technological developments and the increasingly cross-border nature of data storage, the storing of information and computer data is often external to the devices found during searches and more linked to new forms of cloud hosting services with multinational networks. As pointed out by the working Group on undercover investigations and extension of searches in its report[78], in the absence of international standards, States seem to be increasingly pursuing unilateral options and extending searches to computer systems in other jurisdictions (as already concluded by the T-CY Transborder and Cloud Evidence working groups previously) (see corresponding recommendations 14 and 15).[79]

Concl 21 **Extension of a search to computer data whose location is unknown** – Similarly, Parties took a variety of positions as to whether they are permitted by their

[78] A report containing draft options and recommendations for further action by the T-CY on: 1. Undercover investigations by means of a computer system; 2. Extension of searches. The working group presented the report in the 27th T-CY Plenary (29-30 November 2022).

[79] See Cybercrime Convention Committee (T-CY), Ad-hoc Subgroup on Transborder Access and Jurisdiction: Transborder access to data and jurisdiction – Options for further action by the T-CY. Adopted by the 12th Plenary of the T-CY (2-3 December 2014), p. 8. See also Cybercrime Convention Committee (T-CY), T-CY Cloud Evidence Group: Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY (16 September 2016).

domestic law to extend a remote search from their own territory to an unknown location or where it is believed or suspected to most likely be outside the territory. Occasionally Parties indicated that this might be done in practice but that there was no clear underlying legal basis. Some indicated that searches might be extended to an unknown location if the case were sufficiently urgent or important. Other Parties' replies did not address the complexity of the problem, for example, with neither an express legal norm nor uniform jurisprudence to guide the actions of law enforcement. Or, because this issue can be controversial, some Parties seemed hesitant to state their views.

As acknowledged by previous reports of T-CY working groups, an extension of searches cross-border is likely to have a range of policy, legal and other considerations or implications (including the rights of individuals and third parties within the remotely searched territory) for criminal investigations and prosecutions[80]. The increase in remotely stored computer data held outside the territory of a Party means that evidence laws relating to such data may prevent or obstruct their use in criminal prosecutions where not obtained under specific statutory frameworks (such as foreign evidence laws) (see corresponding recommendations 14 and 15).

Concl 22 **Value of developing international mutual understanding on the extension of searches** – Although an extension of searches to a different territory is a measure that goes beyond of the scope of this assessment, this aspect has been of interest to the T-CY for many years.[81] Competent authorities may be unaware of the international effects and issues raised by searches and seizures beyond their territory. They may even expose themselves to legal jeopardy vis-à-vis the targeted country. The adoption of similar or compatible positions among different countries could be important in building an internationally accepted custom and improving international cooperation between the Parties to the Convention. At the same time, similar or compatible positions could protect the Parties' interests and the interests of individuals in their territory from undue access by other States (see corresponding recommendations 14 and 15).

[80] "International cooperation in criminal matters is based on a number of principles, including that of dual criminality or the possibility to refuse cooperation if it is contrary to the public order of the requested State. Transborder access may be used to circumvent such principles." Transborder access and jurisdiction: What are the options? Report of the Transborder Group adopted by the T-CY on 6 December 2012, p. 12.

[81] See the work of the T-CY on transborder access to data, on cloud evidence, or on undercover investigations and extension of searches. https://www.coe.int/en/web/cybercrime/tcy

9.2 Summary of implementation by Parties[82]

Party[83]	Article 19.1	Article 19.2	Article 19.3	Article 19.4	Article 19.5
1. Albania	SP	SP	SP	SP	P (Art. 14)
2. Andorra	GP	GP	GP	GP	P (Art. 14)
3. Argentina	GP/SP	GP	GP/SP	GP	Y
4. Armenia	SP	GP	SP	GP	Y
5. Australia	GP/SP	GP/SP	SP	SP	Y
6. Austria	GP/SP	SP	GP/SP	GP/SP	Y
7. Azerbaijan	GP	GP	GP	GP	Y
8. Belgium	SP	SP	SP	SP	Y
9. Bénin	GP/SP	SP	SP	GP/SP	Y
10. Bosnia and Herzegovina	GP/SP	GP	GP/SP	GP	Y
11. Brazil	GP/SP	GP/SP	GP/SP	GP/SP	Y
12. Bulgaria	SP	SP	SP	GP	Y
13. Cabo Verde	SP	SP	SP	SP	Y
14. Cameroon[84]	GP/SP	N	GP/SP		Y
15. Canada	GP/SP	GP/SP	GP/SP	GP/SP	Y
16. Chile	GP	GP	GP	GP	Y
17. Colombia	GP	GP	GP	GP	Y
18. Costa Rica	GP	GP	GP	GP	Y
19. Croatia	SP	SP	SP	SP	Y
20. Cyprus	GP/SP	GP/SP	GP	N	Y
21. Czech Republic	GP	GP	GP	GP	Y
22. Denmark	GP	GP	GP	GP	Y
23. Dominican Republic	GP/SP	GP	SP	SP	Y
24. Estonia	GP	GP	GP	GP	Y
25. Fiji	SP	SP	SP	SP	Y
26. Finland	SP	SP	GP/SP	SP	Y
27. France	SP	SP	SP	SP	Y
28. Georgia	GP/SP	GP	GP/SP	SP	Y
29. Germany	GP/SP	SP	GP	GP	Y
30. Ghana	GP/SP	GP/SP	GP/SP	GP/SP	Y
31. Greece	GP/SP	GP/SP	GP/SP	N	Y
32. Grenada	SP	GP	SP	SP	Y
33. Hungary	SP	SP	SP	GP/SP	Y
34. Iceland	GP	GP	GP/SP	SP	Y
35. Israel	SP	SP	SP	GP	P (Art. 14)
36. Italy	GP/SP	GP	GP	GP	Y

[82] The Summary of Implementation table addresses whether paragraphs 19.1 - 19.4 are being implemented through the general or specific powers and whether Parties are in line with Article 19.5. Parties are advised to refer to the assessment tables for further details on the implementation of the relevant paragraphs of Article 19 in each Party. Clarifications from some Parties are expected and the table in Section 9.2. may be updated before the T-CY Plenary depending on whether these clarifications are provided.

[83] (GP = general powers
SP = specific powers
Y = in line
P = Partially in line
N = Not implemented)

[84] Clarifications are pending.

Party[83]	Article 19.1	Article 19.2	Article 19.3	Article 19.4	Article 19.5
37. Japan	GP/SP	GP/SP	GP/SP	GP/SP	Y
38. Kiribati[85]	GP/SP	SP			Y
39. Latvia	GP/SP	SP	GP/SP	SP	P (Art. 14)
40. Liechtenstein	GP/SP	GP/SP	GP/SP	GP/SP	Y
41. Lithuania	GP	GP	GP	GP	Y
42. Luxembourg	GP/SP	GP/SP	GP/SP	GP/SP	Y
43. Malta	GP/SP	GP	GP/SP	GP	Y
44. Mauritius	SP	SP	SP	SP	Y
45. Monaco	GP/SP	GP/SP	GP/SP	GP/SP	Y
46. Montenegro	GP/SP	GP/SP	GP/SP	GP/SP	Y
47. Morocco	GP	GP	GP	GP	Y
48. Netherlands	SP	SP	GP/SP	SP	Y
49. Nigeria[86]	GP/SP	GP/SP		GP/SP	Y
50. North Macedonia	GP/SP	GP/SP	GP/SP	GP/SP	Y
51. Norway	GP	GP	GP	SP	Y
52. Panama	SP	SP	SP	GP	Y
53. Paraguay	GP	GP	GP	GP	Y
54. Peru	GP	GP	GP	GP	Y
55. The Philippines	SP	SP	SP	SP	Y
56. Poland	GP/SP	GP/SP	GP/SP	GP	Y
57. Portugal	SP	SP	SP	SP	Y
58. Republic of Moldova	GP	GP	GP/SP	GP	Y
59. Romania	SP	SP	GP/SP	N	Y
60. San Marino	GP	GP	GP	GP	Y
61. Senegal	SP	SP	SP	SP	Y
62. Serbia	GP/SP	GP/SP	GP/SP	GP/SP	Y
63. Sierra Leone	SP	SP	SP	SP	Y
64. Slovak Republic	GP	SP	SP	SP	Y
65. Slovenia	SP	SP	GP/SP	SP	Y
66. Spain	SP	SP	SP	SP	Y
67. Sri Lanka	GP/SP	GP/SP	GP/SP	SP	Y
68. Sweden	GP/SP	GP/SP	GP/SP	GP/SP	Y
69. Switzerland	GP/SP	GP/SP	GP/SP	GP	Y
70. Tonga	GP/SP	GP/SP	GP/SP	SP	Y
71. Tunisia[87]					
72. Türkiye	SP	SP	SP	GP	Y
73. Ukraine	GP/SP	GP	GP/SP	GP	Y
74. United Kingdom	GP/SP	GP/SP	GP/SP	GP/SP	Y
75. United States of America	GP/SP	GP/SP	GP/SP	GP/SP	Y

[85] Clarifications are pending.

[86] Clarifications are pending.

[87] Partial response received. As a result, Tunisia could not be assessed.

9.3 Recommendations

The following recommendations point at actions to be taken by Parties domestically and/or by the T-CY and capacity building programmes:

9.3.1 Recommendations falling primarily under the responsibility of domestic authorities

Rec 1	Parties should ensure that powers of search and seizure are sufficiently detailed and specific to meet the requirements of Article 19 of the Convention. To the extent that the elements of Article 19 cannot be fulfilled by using general or "traditional" procedural powers (such as those that pertain to house searches or the seizure of tangible objects), Parties should give due consideration to establishing powers and procedures specific to stored computer data to meet these obligations. Such specific provisions could also provide greater clarity and enhance legal certainty. Parties may also provide (for example by standard operating procedures or similar guidelines) that judicial authorisations for searches and seizures pertain to specified computer systems or data in order to apply the conditions and safeguards of Article 15.
Rec 2	Parties that do not provide for definitions of computer data (covering computer data, traffic data, subscriber information) in their domestic laws are encouraged to do so based on the relevant definitions contained in the Convention[88] and apply the powers of search and seizure of stored computer data to all types of computer data (subscriber information, traffic and content data) in their stored form.
Rec 3	Parties are encouraged to establish clear guidance for national authorities about how to deal with certain specific situations they may encounter in practice when accessing and securing computer data to ensure a consistent approach, where possible, at domestic level for similar situations. Such situations might include 1) an unopened email message waiting in the mailbox of a service provider until the addressee downloads it, as referred to in para 190 of the Explanatory Report to the Convention, 2) search and seizure of virtual assets, or 3) obtaining data in volatile memory or triage procedures when multiple physical devices are found.
Rec 4	Parties should consider providing for continuous training and guidance of their competent authorities that authorise and carry out search and seizure (including joint trainings for judges, prosecutors and law enforcement officials), especially given the increasing complexity of emerging technologies and how data can be used as electronic evidence of crime. Such training may be complemented by the adoption of guidance documents, where appropriate. Such training activities may be supported, if desired by the Party, by the capacity building programmes of the Council of Europe.
Rec 5	Parties are encouraged to explicitly provide in their legislation for the different conditions and requirements set out in Article 19.2 of the Convention.
Rec 6	Parties should ensure that they have the power to copy data when accessing a computer system. This measure may be preferable to seizing an entire computer system in certain situations (for example, where the data being searched or similarly accessed may be stored on the computer system of a witness who is not actually involved in the wrongdoing or where the data is on a server of a service provider).

[88] This is without prejudice to paragraph 22 of the ER.

Rec 7	In their domestic law or in internal standard operating procedures or similar guidelines, Parties should specify requirements related to maintaining the integrity of the data and chain of custody to ensure that the data were not interfered with (protocols of actions, creating images, hash values, data storage, retention periods). Some of these elements may be found in Article 14 of the Second Additional Protocol (for example, quality and integrity, retention periods, data security, etc.).
Rec 8	Parties should ensure that they have the power to remove the data from a searched computer system or to render them inaccessible under certain conditions.
Rec 9	Parties should ensure that they have the power to order any person with knowledge about the functioning of a computer system, or measures applied to protect its data, to provide, as is reasonable, the information necessary to carry out the actions in Article 19. Amendment of statutes and investigative practices in this respect is urgent. Without prejudice to certain rights under their domestic laws (for example, the right against self-incrimination), Parties are encouraged to consider establishing sanctions if the person refuses to provide necessary cooperation. Parties should restrict the use of this power to provision of information that is reasonable. In particular, Parties should avoid using this power where the disclosure of the password or other security measure would unreasonably threaten the privacy of other users or other data that is not authorised to be searched. In such cases, the provision of the "necessary information" could be the disclosure, in a form that is intelligible and readable, of the actual data that is being sought by the competent authorities.
Rec 10	In the same vein, Parties are encouraged to specify in their domestic law or in internal standard operating procedures or similar guidelines: - grounds that must be met or steps that must be taken to acquire credentials lawfully in accordance with the domestic law of a Party; - how lawfully acquired credentials may be used by their competent authorities (for example, for downloading stored computer data, for undercover activities when controlling the account, or for changing credentials, etc.).
Rec 11	Parties should ensure that their powers to search and seize computer data extend to all types of crimes, consistent with the scope of the Convention under Article 14. In countries where these powers derive from a combination of statutes, the interplay of these statutes should be examined for cases that would fall outside all statutes.
Rec 12	Consistent with obligations under Article 15, Parties should ensure that the measures of search and seizure are applied in accordance with the principle of proportionality, in accordance with relevant principles of their domestic law. The Parties are to apply the conditions and safeguards regardless of whether the power of search and seizure is carried out at the location where the computer system or data is found, or in or from another place. Parties should ensure that applicable legal privileges and immunities are protected. This may include the ability to seek redress for persons claiming such protection. When applying measures of Article 19, to the extent consistent with the public interest, Parties should consider their impact on the rights, responsibilities and legitimate interests of third parties, including service providers, and whether appropriate means can be taken to mitigate such impact.

Rec 13	Some Parties do not have any existing systems in place for conducting searches and seizures of systems consistent with Article 19 in emergency or urgent situations, or they have basic, informal, or ad hoc systems. These Parties are encouraged to review the present Assessment Report to learn how other Parties have approached these situations before they are confronted with an actual emergency or urgency. Parties with more robust systems in place are similarly encouraged to review this Assessment to determine if other Parties may have elements useful to incorporate into their own system. All Parties are reminded that the Second Additional Protocol provides a definition of "emergency" that may provide useful guidance.
Rec 14	Extension of searches to a location known to be foreign or to an unknown location has become an urgent issue that practitioners face. Therefore, Parties should prepare their positions on extensions of searches from their own territory to a location known to be foreign or to an unknown location. In developing such positions, Parties should consider the possible implications of an extension of searches cross-border (policy, legal and other considerations, including the rights of individuals and third parties as well as potential invalidation and suppression of evidence). Possible second judicial authorisations, consultation with or notification of the targeted country, awareness-raising for competent authorities, and amendments to domestic law could be considered in order to mitigate the risks.
Rec 15	Although the measures of extension of searches outside of the territory of a Party or to an unknown location and covert remote access are not specifically provided for in the Convention, Parties may ensure that such measures are subject to the conditions and safeguards that are provided for in Article 15 of the Convention.
Rec 16	Where appropriate, Parties are encouraged to consider sharing their internal standard operating procedures or similar guidelines on the implementation of Article 19 with the Secretariat to make them available with restricted access on the recently developed online platform for exchange of materials, training, and resource sharing on cybercrime and electronic evidence (CYBOX).

9.3.2 Recommendation falling primarily under the responsibility of the T-CY

Rec 17	The T-CY invites the T-CY Bureau to provide the plenary with options for future work on the question of virtual assets and the relevance of the Convention on Cybercrime and its Second Protocol, as decided during the 30th Plenary of the T-CY in June 2024.[89]

9.3.3 Recommendations falling primarily under the responsibility of Council of Europe

Rec 18	The Cybercrime Programme Office of the Council of Europe (C-PROC) should support reforms of legislation, training and specialisation (including specialised authorities) on search and seizure of stored computer data.
Rec 19	The Council of Europe (T-CY Secretariat and C-PROC) should make available, with restricted access, materials on the implementation of Article 19 of the Convention shared by Parties on the recently developed online platform for exchange of materials, training, and resource sharing on cybercrime and electronic evidence (CYBOX).

[89] https://rm.coe.int/t-cy-2024-6-plen30-rep-v4final/1680b07f1c

9.4 Follow up

The Parties are invited to inform the T-CY and its Secretariat of measures taken and examples of good practices at any time.

Parties are invited to provide an update on follow up to applicable recommendations falling under the responsibility of domestic authorities to report back to the T-CY no later than 18 months from adoption of this report on measures taken to permit the T-CY, in line with the Rules of Procedure (Article 2.1.g), to review progress made.

The Council of Europe Secretariat is requested to follow up on recommendations falling under its responsibility and to report back to the T-CY within 18 months of adoption of the report.

The T-CY will then review progress made.

10 APPENDIX

10.1 Examples of domestic legal provisions

10.1.1 Argentina

Input available for download here.

10.1.2 Austria

Input available for download here and here.

10.1.3 Canada

"Peace Officer"

peace officer includes

- **(a)** a mayor, warden, reeve, sheriff, deputy sheriff, sheriff's officer and justice of the peace,
- **(b)** a member of the Correctional Service of Canada who is designated as a peace officer pursuant to Part I of the *Corrections and Conditional Release Act*, and a warden, deputy warden, instructor, keeper, jailer, guard and any other officer or permanent employee of a prison other than a penitentiary as defined in Part I of the *Corrections and Conditional Release Act*,
- **(c)** a police officer, police constable, bailiff, constable, or other person employed for the preservation and maintenance of the public peace or for the service or execution of civil process,
- **(c.1)** a designated officer as defined in section 2 of the *Integrated Cross-border Law Enforcement Operations Act*, when
    - **(i)** participating in an integrated cross-border operation, as defined in section 2 of that Act, or
    - **(ii)** engaging in an activity incidental to such an operation, including travel for the purpose of participating in the operation and appearances in court arising from the operation,
- **(d)** an officer within the meaning of the *Customs Act*, the *Excise Act* or the *Excise Act, 2001*, or a person having the powers of such an officer, when performing any duty in the administration of any of those Acts,
- **(d.1)** an officer authorized under subsection 138(1) of the *Immigration and Refugee Protection Act*,
- **(e)** a person designated as a fishery guardian under the *Fisheries Act* when performing any duties or functions under that Act and a person designated as a fishery officer under the *Fisheries Act* when performing any duties or functions under that Act or the *Coastal Fisheries Protection Act*,
- **(f)** the pilot in command of an aircraft
    - **(i)** registered in Canada under regulations made under the *Aeronautics Act*, or
    - **(ii)** leased without crew and operated by a person who is qualified under regulations made under the *Aeronautics Act* to be registered as owner of an aircraft registered in Canada under those regulations,

while the aircraft is in flight, and

- **(g)** officers and non-commissioned members of the Canadian Forces who are
    - **(i)** appointed for the purposes of section 156 of the *National Defence Act*, or

(ii) employed on duties that the Governor in Council, in regulations made under the *National Defence Act* for the purposes of this paragraph, has prescribed to be of such a kind as to necessitate that the officers and non-commissioned members performing them have the powers of peace officers; (*agent de la paix*)

10.1.4 Czech Republic

Input available for download here.

10.1.5 Estonia

Extracts from Criminal Procedure Code
https://www.riigiteataja.ee/en/eli/ee/504042023004/consolide/current

§ 63. Item of evidence

(1) 'Item of evidence' means a statement or testimony of the suspect, accused, victim, witness or specialist witness, an expert's report, the statement or testimony given by an expert when providing clarifications concerning their report, an item of physical evidence, a report of an investigative or a covert operation, the record or video recording of a trial or hearing or the report or video recording of an investigative or a covert operation, and also any other document, as well as any photograph, footage or other data recording.

(1^1) The presentation, as evidence in criminal proceedings, of any information collected under the Security Authorities Act is decided by the Prosecutor General, having regard to the restrictions mentioned in subsection 2 of § 1261 and subsection 2 of § 1267 of this Code.

(2) Items of evidence not listed in subsection 1 of this section may also be used to prove the facts at issue in criminal proceedings, except where they have been obtained by a criminal offence or by means of violating a fundamental right.

§ 64. General conditions for the collection of evidence

(1) Evidence is collected in a manner which does not offend the honour and dignity of those participating in its collection, does not endanger the life or health of such participants and does not cause unjustified pecuniary harm. It is prohibited to collect evidence by torturing a person or by subjecting them to violence in any other way, or by using means which affects their faculty of memory, or by treating them in a manner that degrades human dignity.

(2) If, in the course of a search or physical examination of a person, or of the taking of material for comparison, it is necessary to reveal the body of the person, the official of the investigative authority, the prosecutor and any other participants in the corresponding procedural operation, except health care professionals and forensic pathologists, must be of the same sex as the person.

(3) If technical equipment is to be used to take the evidence, this is notified in advance to the participants in the corresponding procedural operation and the purpose of using the equipment is explained to them.

(4) [Repealed – RT I, 23.02.2011, 1 – entry into force 01.09.2011]

(5) Where this is needed, participants of a procedural operation are cautioned that, under § 214 of this Code, disclosure of information relating to pre-trial proceedings is not allowed.

(6) The taking of evidence by covert operations is regulated by Chapter 31 of this Code.

§ 83. Aim of inspection and objects of inspection

(1) The aim of an inspection is to collect information required for resolving the criminal case, to detect the indicia of a criminal offence and to seize any objects that are to be used as physical evidence.

(2) The objects of inspection are:

1) the scene of events;

2) the corpse;

3) a document, another object or an item of physical evidence;

4) where a physical examination is to be conducted, the person or the postal or telegraphic item to be examined.

(3) Where explanations from the suspect, accused, witness, specialist witness or victim are conducive to ensuring the comprehensiveness, exhaustiveness and objectivity of the inspection, the person is summoned to attend the inspection.

§ 86. Inspection of document, another object or an item of physical evidence

(1) When inspecting a document or another object, the indicia of a criminal offence and any other characteristic features that are needed for resolving the criminal case and that constitute grounds for using the object in question as an item of physical evidence are ascertained.

(2) Where further examination of a document, thing or other object that appears as an item of physical evidence is needed, an inspection of the item of physical evidence is performed.

§ 91. Search

(1) The aim of a search is to find, in a building, a room, a vehicle or an enclosed area, an object to be confiscated or used as an item of physical evidence, or a document, thing or person needed for resolving the criminal case, or property to be attached in criminal proceedings, or a corpse, or to apprehend a person who has been declared a fugitive from justice. A search may be conducted provided there is a reasonable suspicion that what is searched for is located at the place to be searched.

(2) Unless otherwise provided by this Code, a search may be conducted on an application of the Prosecutor's Office under a warrant from the pre-trial investigation judge or from the court. The order by which the pre-trial investigation judge or the court disposes of such an application may take the form of a note made on the application.

(3) A search may be conducted based on a warrant from the Prosecutor's Office, except for a search at a notary's office or at the office of a law firm or at the premises of a person processing information for journalistic purposes, provided there is reason to believe that the suspect is using the premises or vehicle to be searched, or used those premises or that vehicle, at the time of the criminal event or during pre-trial proceedings, and the person is suspected of having committed a criminal offence mentioned in subsection 2 of § 1262 of this Code.

(4) A search warrant states:

1) as the aim of the search, what the search is for (hereinafter, 'the object searched for');

2) the reasons for the search;

3) the place at which the search is conducted.

(5) In a situation of urgency, if it is not possible to issue a search warrant at a proper time, a search may be conducted, on conditions provided by subsection 3 of this section, based on an authorisation of the Prosecutor's Office provided in a form reproducible in writing.

(6) When a search is conducted on the grounds provided by subsections 3 and 5 of this section, this must be notified, through the Prosecutor's Office, to the pre-trial investigation judge during the first working day following commencement of the search. The judge decides, by an order which may be made as a note on the warrant from the Prosecutor's Office, whether or not to declare the search permissible.

(7) During the lead-in to a search, the search warrant is presented to the person at whose premises the search is performed, or to a full-age member of their family, or to a representative of the legal person or of the State or municipal authority at whose premises the search is performed. Signed acknowledgement of such presentation is obtained on the warrant from the person, family member or representative. In a situation mentioned in subsection 5 of this section, the circumstances mentioned in subsection 4 of this section, and the reasons for conducting the search as a matter of urgency, are explained to the person, family member or representative. Signed acknowledgement of such explanation is obtained on the search report from the person, family member or representative. Where the relevant person or representative is not present, participation of a representative of the municipality must be arranged.

(8) When a search is conducted at the office of a notary or of a law firm, the notary or the attorney at whose premises the search is performed must be in attendance. If the notary or attorney cannot attend the search, it must be attended by the person who stands in for the notary or by another attorney who provides legal services through the same firm or, where this is impossible, by another notary or another attorney.

(9) During the lead-in to a search, an invitation is made to hand over the object searched for or to show the place where a corpse has been hidden or where a person who has been declared

a fugitive is hiding. If the invitation is not acceded to or if there is reason to believe that it has only been followed in part, search operations are conducted.
(10) In the course of a search, any objects that are subject to confiscation or that clearly represent items of evidence in criminal proceedings may be seized, provided these were discovered without any search operations, in a clearly visible place, or in the course of reasonable search operations undertaken to find the objects searched for.

§ 126[4]. Granting an authorisation for a covert operation
(1) A covert operation may be conducted when this is authorised in writing by the Prosecutor's Office or by the pre-trial investigation judge. The pre-trial investigation judge resolves the grant of such an authorisation by an order on the basis of a reasoned application from the Prosecutor's Office. A reasoned application of the Prosecutor's Office is considered by the pre-trial investigation judge without delay and an authorisation to conduct the covert operation in question is granted or refused by an order.
(2) In situations of urgency, a covert operation that requires an authorisation from the Prosecutor's Office may be conducted with such an authorisation being issued in a reproducible form. A written authorisation is issued within 24 hours following commencement of the operation.
(3) Where an immediate danger to the life, physical integrity, physical freedom or a high-value property interest of a person is involved, and where it is not possible to apply for or to issue a relevant authorisation at a proper time, a covert operation that requires authorisation from the court may be conducted, in a situation of urgency, with such an authorisation being issued in a reproducible form. A written application is filed and a corresponding authorisation issued within 24 hours following commencement of the operation.
(4) An authorisation issued in a situation of urgency in a reproducible form must contain the following information:
1) the issuer of the authorisation;
2) the date and time of issue of the authorisation;
3) the covert operation for which the authorisation is issued;
4) where it is known, the name of the person in respect of whom the covert operation is to be conducted;
5) the time limit of the permission for covert operations.
(5) Where, to **conduct a covert operation** or to place or remove any technical means required for such an operation, **covert entry** needs to be made to a building, room, vehicle, an enclosed area or a **computer system**, the Prosecutor's Office applies for and obtains a corresponding separate authorisation from the pre-trial investigation judge.
(6) The duration of covert operations conducted with respect to a particular person on the grounds provided by clauses 1, 2 and 4 of subsection 1 of § 126[2] of this Code in the same proceedings must not exceed one year. In exceptional situations, the Prosecutor General may authorise, or apply to the court for authorisation to conduct, covert operations for more than one year. In a criminal case dealt with under Council Regulation (EU) 2017/1939, the relevant authorisation is granted, or application made, by a European Prosecutor or a European Delegated Prosecutor.

§ 126[5]. Covert surveillance, covert collection of samples for comparison and conduct of initial investigations, covert examination and substitution of an object
(1) For conducting covert surveillance of a person, an object or area, for covert collection of samples for comparison and for conducting initial investigations, and for covert examination or substitution of an object, the Prosecutor's Office grants an authorisation for up to two months. The Prosecutor's Office may extend the time limit of the authorisation by up to two months at a time.
(2) In the course of covert operations mentioned in this section, collected information is – where this is needed – video recorded, photographed or copied or recorded by any other method.

10.1.6 Finland

Input available for download here.

10.1.7 Georgia

Input available for download here.

10.1.8 Germany

Input available for download here.

10.1.9 Hungary

Attachment_Court_ decisions.docx

10.1.10 Kiribati

Cybercrime Act 2021

10.1.11 Lithuania

Input available here, here, here and here.

10.1.12 Norway

Input available here.

10.1.13 Paraguay

Input available here and here.

10.1.14 Republic of Moldova

Article 11. Inviolability of the person (CPC)
(1) Individual liberty and security of person are inviolable.
....
(7) Search, bodily examination and other procedural actions affecting the inviolability of the person may be carried out without the consent of the person or his legal representative only under the conditions of this Code.
Article 12. Inviolability of the home (CPC)
(1) Inviolability of the home is guaranteed by law. In the course of criminal proceedings, no one shall be entitled to enter the domicile against the will of the persons residing or having premises therein, except in the cases and manner provided for in this Code.
(2) Searches, house searches, and other criminal pursuits at home may be ordered and carried out under a judicial warrant, except in the cases and manner provided for in this Code. In case of carrying out procedural actions without a judicial warrant, the body authorized to carry out such actions shall, immediately, but not later than 24 hours after the completion of the action, submit the respective materials to the court for review of the legality of such actions.

Article 13. Inviolability of property (CPC)
(1) A natural or legal person may not be arbitrarily deprived of the right of ownership. No one may be deprived of his property except for reasons of public utility and in accordance with this Code and the general principles of international law.
(2) Property may be seized only on the basis of a court decision.
(3) Property seized in the course of the proceedings shall be described in the minutes of the proceedings and the person from whom it was seized shall be given a copy of the minutes of the proceedings.

Article 14. Secrecy of correspondence (CPC)
(1) The right to secrecy of letters, telegrams, other postal items, telephone conversations and other lawful means of communication shall be guaranteed by the State. In the course of criminal proceedings, no one may be deprived of or restricted in this right.
(2) Limitation of the right referred to in paragraph (1) shall be allowed only on the basis of a judicial warrant issued under the conditions of this Code.

Article 15. Inviolability of privacy (CPC)
(1) Everyone has the right to inviolability of privacy, to the confidentiality of intimate and family life and to the protection of personal honour and dignity. In the course of criminal proceedings, no one shall have the right to arbitrarily and illegitimately intrude into a person's private life.
(2) In the conduct of procedural actions, information about the private and intimate life of the person may not be gathered unnecessarily. At the request of the prosecution body and the court, the participants in the procedural actions shall be obliged not to disclose such information and a written undertaking shall be made about it. The processing of personal data in criminal proceedings shall be carried out in accordance with the provisions of the Law No.133 of 8 July 2011 on the protection of personal data.
(3) Persons from whom the prosecuting authority requests information about private and intimate life are entitled to be satisfied that this information is administered in a specific criminal case. The person shall not be entitled to refuse to provide information about his or her private and intimate life or that of other persons under the pretext of the inviolability of privacy, but he or she shall be entitled to ask the prosecuting body for an explanation of the necessity of obtaining such information, with the inclusion of the explanation in the minutes of the respective procedural action.
(4) Evidence confirming information about the person's private and intimate life shall, at the request of the person, be examined in a closed court session.
(5) The damage caused to the person in the course of criminal proceedings by violation of his/her private and intimate life shall be compensated in the manner established by the legislation in force.

Article 127. Persons present when objects and documents are searched or seized
(1) If necessary, the *interpreter or specialist* may be present during the search or seizure of objects and documents.
(2) The presence of the person to be searched or seized or of adult members of his/her family or of those representing the interests of the person concerned shall be ensured during the search or seizure of objects and documents. If the presence of these persons is impossible, *the representative of the executive authority of the local public administration shall be invited*.
(3) The seizing of objects and documents or the search of premises of institutions, enterprises, organisations and military units shall be carried out in the presence of the representative concerned.
(4) The persons whose objects and documents are searched or seized, as well as specialists, interpreters, representatives, defenders, have the right to be present at all actions of the prosecution body/law enforcement and to make objections and statements in relation thereto, which shall be recorded in the minutes.

(5) For the purpose of ensuring security, the prosecution authorities/law enforcement may involve subdivisions of the institutions referred to in Article 56(1) or other institutions. The identity of the persons involved by the prosecution authorities/ law enforcement for the purpose of ensuring security may be concealed and/or disguised, which shall be recorded in the minutes.
(6) The person who is searched or whose objects and documents shall be seized, shall have the right to record by audio-visual means these actions, informing the prosecution body / law enforcement of this fact.
(7) If the person searched requests the presence of a *defence counsel (attorney)*, the proceedings shall be interrupted until the defence counsel (attorney) is present, but for no longer than 2 hours. In case of urgency caused by the risk of loss, alteration or destruction of evidence or danger to the safety of the person being searched or other persons, the search shall continue, with reasons being stated in the minutes.

Article 300. Scope of judicial supervision

(1) The investigating judge shall examine the prosecutor's requests for authorisation to carry out criminal prosecution actions, special investigative measures and the application of procedural measures of constraint limiting the constitutional rights and freedoms of the person, as well as requests for the completion of criminal proceedings in the absence of the accused.
…

Article 301. Prosecution proceedings conducted with the authorisation of the investigating judge
(1) With the authorization of the investigating judge, criminal prosecution actions related to the limitation of inviolability of the person, domicile, limitation of secrecy of correspondence, telephone calls, telegraphic and other communications, completion of criminal prosecution in the absence of the accused, as well as other actions provided by law shall be carried out
(2) Prosecution actions in the form of search, the scene investigation in the domicile and seizure of property following a search may be carried out, by way of exception, without the authorisation of the investigating judge, on the basis of a reasoned order of the public prosecutor, in cases of flagrante delicto and in cases which do not allow for postponement. The examining magistrate must be informed of the carrying out of these prosecution actions *within 24 hours*, and for the purpose of control, he presents the materials of the criminal case in which the prosecution actions carried out are substantiated. If there are sufficient grounds, the investigating judge shall, by a reasoned decision, declare the prosecution action lawful or, where appropriate, unlawful.
…

Article 306. Court warrant on carrying out criminal prosecution actions, special investigative measures or on applying procedural measures of constraint

The court decision on the carrying out of the prosecution, special investigative measures or on the application of procedural measures of constraint shall indicate: the date and place of its drawing up, the name and surname of the investigating judge, the person in charge and the body which submitted the request, the body carrying out the prosecution, the special investigative measures or applying procedural measures of constraint, indicating the purpose of carrying out these actions or measures and the person to whom they refer, as well as a mention of the authorisation of the action or its rejection in case of objections of the defence counsel, the legal representative, the suspect, the accused, the defendant, the reasons for their admission or non-admission to the application of the measure of constraint, the term for which the action is authorised, **the person in charge or the body authorised to execute the warrant (court order)**, the signature of the investigating judge certified with the stamp of the court.

Article 540/2. Joint investigation teams
(1) The competent authorities of at least two States may, by mutual agreement, set up a joint investigation team for a specific purpose and for a limited period of time, which may be

extended with the agreement of all parties, for the purpose of conducting criminal proceedings in one or more of the States setting up the team. The composition of the joint investigation team shall be decided by mutual agreement.

- Chapter IX (art.531-540[1] CPC)
INTERNATIONAL LEGAL ASSISTANCE IN CRIMINAL MATTERS

Article 533. Scope of legal aid
(1) International legal assistance may be requested or granted in the execution of certain procedural activities provided for by the criminal procedure legislation of the Republic of Moldova and of the foreign State concerned in particular:
…
3) conducting the scene investigation, **search, seizure of objects and documents and their transmission abroad**, **seizure**, confrontation, presentation for recognition, identification of telephone subscribers, interception of communications, **carrying out forensic expertise**, confiscation of property derived from the commission of crimes and other criminal prosecution actions provided for in this Code;
…

Art.536 Rogatory letters
(1) The prosecuting authority or court, if it considers necessary to perform prosecution actions *in the territory of a foreign State*, shall address itself by rogatory letter to the prosecuting authority or court of that State, or to an international criminal court in accordance with the international treaty to which the Republic of Moldova is a party or through diplomatic channels, under conditions of reciprocity.

Art.540/1. Search, seizure, removal of objects or documents, seizure and confiscation

Rogatory letters requesting the search, seizure or remittance of objects or documents, as well as seizure or confiscation shall be executed in accordance with the law of the Republic of Moldova.

10.1.15 United States of America

Federal Rules of Criminal Procedure – Rule 17
(a) Content.—A subpoena must state the court's name and the title of the proceeding, include the seal of the court, and command the witness to attend and testify at the time and place the subpoena specifies. The clerk must issue a blank subpoena—signed and sealed—to the party requesting it, and that party must fill in the blanks before the subpoena is served.

(b) Defendant Unable to Pay.—Upon a defendant's ex parte application, the court must order that a subpoena be issued for a named witness if the defendant shows an inability to pay the witness's fees and the necessity of the witness's presence for an adequate defense. If the court orders a subpoena to be issued, the process costs and witness fees will be paid in the same manner as those paid for witnesses the government subpoenas.

(c) Producing Documents and Objects.
(1) In General.—A subpoena may order the witness to produce any books, papers, documents, data, or other objects the subpoena designates. The court may direct the witness to produce the designated items in court before trial or before they are to be offered in evidence. When the items arrive, the court may permit the parties and their attorneys to inspect all or part of them.
(2) Quashing or Modifying the Subpoena.—On motion made promptly, the court may quash or modify the subpoena if compliance would be unreasonable or oppressive.

(3) Subpoena for Personal or Confidential Information About a Victim.—After a complaint, indictment, or information is filed, a subpoena requiring the production of personal or confidential information about a victim may be served on a third party only by court order. Before entering the order and unless there are exceptional circumstances, the court must require giving notice to the victim so that the victim can move to quash or modify the subpoena or otherwise object.

(d) Service.—A marshal, a deputy marshal, or any nonparty who is at least 18 years old may serve a subpoena. The server must deliver a copy of the subpoena to the witness and must tender to the witness one day's witness-attendance fee and the legal mileage allowance. The server need not tender the attendance fee or mileage allowance when the United States, a federal officer, or a federal agency has requested the subpoena.

(e) Place of Service.—
(1) In the United States.—A subpoena requiring a witness to attend a hearing or trial may be served at any place within the United States.
(2) In a Foreign Country.—If the witness is in a foreign country, 28 U.S.C. §1783 governs the subpoena's service.

(f) Issuing a Deposition Subpoena.—

(1) Issuance.—A court order to take a deposition authorises the clerk in the district where the deposition is to be taken to issue a subpoena for any witness named or described in the order.
(2) Place.—After considering the convenience of the witness and the parties, the court may order—and the subpoena may require—the witness to appear anywhere the court designates.

(g) Contempt.—The court (other than a magistrate judge) may hold in contempt a witness who, without adequate excuse, disobeys a subpoena issued by a federal court in that district. A magistrate judge may hold in contempt a witness who, without adequate excuse, disobeys a subpoena issued by that magistrate judge as provided in 28 U.S.C. §636(e).

(h) Information Not Subject to a Subpoena.—No party may subpoena a statement of a witness or of a prospective witness under this rule. Rule 26.2 governs the production of the statement.

Federal Rules of Criminal Procedure – Rule 41
(a) Scope and Definitions.—
(1) Scope.—This rule does not modify any statute regulating search or seizure, or the issuance and execution of a search warrant in special circumstances.
(2) Definitions.—The following definitions apply under this rule:
(A) "Property" includes documents, books, papers, any other tangible objects, and information.
(B) "Daytime" means the hours between 6:00 a.m. and 10:00 p.m. according to local time.
(C) "Federal law enforcement officer" means a government agent (other than an attorney for the government) who is engaged in enforcing the criminal laws and is within any category of officers authorised by the Attorney General to request a search warrant.
(D) "Domestic terrorism" and "international terrorism" have the meanings set out in 18 U.S.C. §2331.
(E) "Tracking device" has the meaning set out in 18 U.S.C. §3117 (b).

(b) Venue for a Warrant Application.—At the request of a federal law enforcement officer or an attorney for the government:

(1) a magistrate judge with authority in the district—or if none is reasonably available, a judge of a state court of record in the district—has authority to issue a warrant to search for and seize a person or property located within the district;
(2) a magistrate judge with authority in the district has authority to issue a warrant for a person or property outside the district if the person or property is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed;
(3) a magistrate judge—in an investigation of domestic terrorism or international terrorism—with authority in any district in which activities related to the terrorism may have occurred has authority to issue a warrant for a person or property within or outside that district;
(4) a magistrate judge with authority in the district has authority to issue a warrant to install within the district a tracking device; the warrant may authorise use of the device to track the movement of a person or property located within the district, outside the district, or both; and
(5) a magistrate judge having authority in any district where activities related to the crime may have occurred, or in the District of Columbia, may issue a warrant for property that is located outside the jurisdiction of any state or district, but within any of the following:
(A) a United States territory, possession, or commonwealth;
(B) the premises—no matter who owns them—of a United States diplomatic or consular mission in a foreign state, including any appurtenant building, part of a building, or land used for the mission's purposes; or
(C) a residence and any appurtenant land owned or leased by the United States and used by United States personnel assigned to a United States diplomatic or consular mission in a foreign state.
(6) a magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if:
(A) the district where the media or information is located has been concealed through technological means; or
(B) in an investigation of a violation of 18 U.S.C. § 1030(a)(5), the media are protected computers that have been damaged without authorisation and are located in five or more districts.

(c) Persons or Property Subject to Search or Seizure.—A warrant may be issued for any of the following:
(1) evidence of a crime;
(2) contraband, fruits of crime, or other items illegally possessed;
(3) property designed for use, intended for use, or used in committing a crime; or
(4) a person to be arrested or a person who is unlawfully restrained.

(d) Obtaining a Warrant.—
(1) In General.—After receiving an affidavit or other information, a magistrate judge—or if authorised by Rule 41(b), a judge of a state court of record—must issue the warrant if there is probable cause to search for and seize a person or property or to install and use a tracking device.
(2) Requesting a Warrant in the Presence of a Judge.—
(A) Warrant on an Affidavit.—When a federal law enforcement officer or an attorney for the government presents an affidavit in support of a warrant, the judge may require the affiant to appear personally and may examine under oath the affiant and any witness the affiant produces.
(B) Warrant on Sworn Testimony.—The judge may wholly or partially dispense with a written affidavit and base a warrant on sworn testimony if doing so is reasonable under the circumstances.

(C) Recording Testimony.—Testimony taken in support of a warrant must be recorded by a court reporter or by a suitable recording device, and the judge must file the transcript or recording with the clerk, along with any affidavit.

(3) Requesting a Warrant by Telephonic or Other Reliable Electronic Means.—In accordance with Rule 4.1, a magistrate judge may issue a warrant based on information communicated by telephone or other reliable electronic means.

(e) Issuing the Warrant.—

(1) In General.—The magistrate judge or a judge of a state court of record must issue the warrant to an officer authorised to execute it.

(2) Contents of the Warrant.—

(A) Warrant to Search for and Seize a Person or Property.—Except for a tracking-device warrant, the warrant must identify the person or property to be searched, identify any person or property to be seized, and designate the magistrate judge to whom it must be returned. The warrant must command the officer to:

(i) execute the warrant within a specified time no longer than 14 days;

(ii) execute the warrant during the daytime, unless the judge for good cause expressly authorises execution at another time; and

(iii) return the warrant to the magistrate judge designated in the warrant.

(B) Warrant Seeking Electronically Stored Information.—A warrant under Rule 41(e)(2)(A) may authorise the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorises a later review of the media or information consistent with the warrant. The time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review.

(C) Warrant for a Tracking Device.—A tracking-device warrant must identify the person or property to be tracked, designate the magistrate judge to whom it must be returned, and specify a reasonable length of time that the device may be used. The time must not exceed 45 days from the date the warrant was issued. The court may, for good cause, grant one or more extensions for a reasonable period not to exceed 45 days each. The warrant must command the officer to:

(i) complete any installation authorised by the warrant within a specified time no longer than 10 days;

(ii) perform any installation authorised by the warrant during the daytime, unless the judge for good cause expressly authorises installation at another time; and

(iii) return the warrant to the judge designated in the warrant.

(f) Executing and Returning the Warrant.—

(1) Warrant to Search for and Seize a Person or Property.—

(A) Noting the Time.—The officer executing the warrant must enter on it the exact date and time it was executed.

(B) Inventory.—An officer present during the execution of the warrant must prepare and verify an inventory of any property seized. The officer must do so in the presence of another officer and the person from whom, or from whose premises, the property was taken. If either one is not present, the officer must prepare and verify the inventory in the presence of at least one other credible person. In a case involving the seizure of electronic storage media or the seizure or copying of electronically stored information, the inventory may be limited to describing the physical storage media that were seized or copied. The officer may retain a copy of the electronically stored information that was seized or copied.

(C) Receipt.—The officer executing the warrant must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken or leave a copy of the warrant and receipt at the place where the officer took the property. For a warrant to use remote access to search electronic storage media and seize or copy electronically stored information, the officer must make reasonable efforts to serve a

copy of the warrant and receipt on the person whose property was searched or who possessed the information that was seized or copied. Service may be accomplished by any means, including electronic means, reasonably calculated to reach that person. **(D) Return.—**The officer executing the warrant must promptly return it—together with a copy of the inventory—to the magistrate judge designated on the warrant. The officer may do so by reliable electronic means. The judge must, on request, give a copy of the inventory to the person from whom, or from whose premises, the property was taken and to the applicant for the warrant.

(2) Warrant for a Tracking Device.—

(A) Noting the Time.—The officer executing a tracking-device warrant must enter on it the exact date and time the device was installed and the period during which it was used.

(B) Return.—Within 10 days after the use of the tracking device has ended, the officer executing the warrant must return it to the judge designated in the warrant. The officer may do so by reliable electronic means.

(C) Service.—Within 10 days after the use of the tracking device has ended, the officer executing a tracking-device warrant must serve a copy of the warrant on the person who was tracked or whose property was tracked. Service may be accomplished by delivering a copy to the person who, or whose property, was tracked; or by leaving a copy at the person's residence or usual place of abode with an individual of suitable age and discretion who resides at that location and by mailing a copy to the person's last known address. Upon request of the government, the judge may delay notice as provided in Rule 41(f)(3).

(3) Delayed Notice.—Upon the government's request, a magistrate judge—or if authorised by Rule 41(b), a judge of a state court of record—may delay any notice required by this rule if the delay is authorised by statute.

(g) Motion to Return Property.—A person aggrieved by an unlawful search and seizure of property or by the deprivation of property may move for the property's return. The motion must be filed in the district where the property was seized. The court must receive evidence on any factual issue necessary to decide the motion. If it grants the motion, the court must return the property to the movant, but may impose reasonable conditions to protect access to the property and its use in later proceedings.

(h) Motion to Suppress.—A defendant may move to suppress evidence in the court where the trial will occur, as Rule 12 provides.

(i) Forwarding Papers to the Clerk.—The magistrate judge to whom the warrant is returned must attach to the warrant a copy of the return, of the inventory, and of all other related papers and must deliver them to the clerk in the district where the property was seized.

18 U.S.C. § 3103a

(a) In General.—In addition to the grounds for issuing a warrant in section 3103 of this title, a warrant may be issued to search for and seize any property that constitutes evidence of a criminal offense in violation of the laws of the United States.

(b) Delay.—With respect to the issuance of any warrant or court order under this section, or any other rule of law, to search for and seize any property or material that constitutes evidence of a criminal offense in violation of the laws of the United States, any notice required, or that may be required, to be given may be delayed if—

(1) the court finds reasonable cause to believe that providing immediate notification of the execution of the warrant may have an adverse result (as defined in section 2705, except if the adverse results consist only of unduly delaying a trial);

(2) the warrant prohibits the seizure of any tangible property, any wire or electronic communication (as defined in section 2510), or, except as expressly provided in chapter 121, any stored wire or electronic information, except where the court finds reasonable necessity for the seizure; and

(3) the warrant provides for the giving of such notice within a reasonable period not to exceed 30 days after the date of its execution, or on a later date certain if the facts of the case justify a longer period of delay.

(c) Extensions of Delay.—Any period of delay authorised by this section may be extended by the court for good cause shown, subject to the condition that extensions should only be granted upon an updated showing of the need for further delay and that each additional delay should be limited to periods of 90 days or less, unless the facts of the case justify a longer period of delay.

(d) Reports.—

(1) Report by judge.—Not later than 30 days after the expiration of a warrant authorising delayed notice (including any extension thereof) entered under this section, or the denial of such warrant (or request for extension), the issuing or denying judge shall report to the Administrative Office of the United States Courts—

(A) the fact that a warrant was applied for;

(B) the fact that the warrant or any extension thereof was granted as applied for, was modified, or was denied;

(C) the period of delay in the giving of notice authorised by the warrant, and the number and duration of any extensions; and

(D) the offense specified in the warrant or application.

(2) Report by administrative office of the united states courts.—Beginning with the fiscal year ending September 30, 2007, the Director of the Administrative Office of the United States Courts shall transmit to Congress annually a full and complete report summarizing the data required to be filed with the Administrative Office by paragraph (1), including the number of applications for warrants and extensions of warrants authorising delayed notice, and the number of such warrants and extensions granted or denied during the preceding fiscal year.

(3) Regulations.—The Director of the Administrative Office of the United States Courts, in consultation with the Attorney General, is authorised to issue binding regulations dealing with the content and form of the reports required to be filed under paragraph (1).

10.2 Overview of replies to the questionnaire[90]

1.1 Please provide an overview of the legal basis for the search and seizure of stored computer data in your country.	Countries that have adopted specific powers[91] for the search and seizure of stored computer data, that may also complement general powers.	Albania, Argentina, Armenia, Australia, Austria, Belgium, Bénin, Brazil, Bulgaria, Cabo Verde, Cameroon, Canada, Croatia, Cyprus, Dominican Republic, Fiji, Finland, France, Georgia, Germany, Ghana, Greece, Grenada, Hungary, Israel, Italy, Japan, Kiribati, Latvia, Liechtenstein, Luxembourg, Malta, Mauritius, Monaco, Montenegro, Netherlands, Nigeria, North Macedonia, Panama, Philippines, Poland, Portugal, Romania, Senegal, Serbia, Sierra Leone, Slovak Republic, Slovenia, Spain, Sri Lanka, Sweden, Switzerland, Tonga, Türkiye, United Kingdom, USA
	Countries that largely rely only on general powers[92] of their laws but may in some instances have practices or operating procedures to apply those for the search and seizure of stored computer data	Andorra, Azerbaijan, Bosnia and Herzegovina, , Chile, Colombia, Costa Rica, Czech Republic, Denmark, Estonia, Iceland, Lithuania, Morocco, Norway, Peru, Paraguay, Republic of Moldova, San Marino, Ukraine
1.2 Do the powers for the search and seizure of stored computer data apply only to offences against or by means of computers or also other offences under your domestic law where evidence is on a computer system?	All offences where evidence is on a computer system	Argentina, Armenia, Australia, Austria, Azerbaijan, Belgium, Bénin, Bosnia and Herzegovina, Brazil, Bulgaria, Cabo Verde, Cameroon, Chile, Colombia, Costa Rica, Croatia, Cyprus, Czech Republic, Denmark, Dominican Republic, Estonia, Fiji, Finland, France, Georgia, Germany, Ghana, Greece, Grenada, Hungary, Iceland, Japan, Kiribati, Liechtenstein, Lithuania, Luxembourg, Malta, Mauritius, Moldova, Monaco, Montenegro, Morocco, Netherlands, Nigeria, North Macedonia, Norway, Panama, Peru, Philippines, Poland, Portugal, Romania, San Marino, Senegal, Serbia, Sierra Leone, Slovak Republic, Slovenia, Spain, Sri Lanka, Sweden, Switzerland, Tonga, Türkiye, Ukraine, United Kingdom, USA

[90] Readers must not rely on the matrix by itself, because it was not possible to reflect ambiguities and nuances of countries' laws in a simple chart.

[91] "specific power" may be any statute, law, ordinance, rule, regulation with a binding force under domestic law specifically providing for search and seizure of computer data and systems.

[92] "general power" may be any statute, law, ordinance, rule, regulation with a binding force that does not mention search and seizure of computer data and systems specifically.

	Certain offences where evidence is on a computer system	Albania, Andorra, Israel, Latvia
	Only offences against or by means of computers	
1.3 What do you consider to comprise "stored computer data"?	Specific definition in a text	Australia, Bulgaria, Cabo Verde, Chile, Finland, Germany, Lithuania, Malta, Moldova, Netherlands, Senegal, Sri Lanka, Switzerland
	No specific definition in a text	Andorra, Argentina, Armenia, Austria, Azerbaijan, Belgium, Bénin, Bosnia and Herzegovina, Brazil, Bulgaria, Cameroon, Canada, Costa Rica, Croatia, Cyprus, Denmark, Dominican Republic, Estonia, Fiji, France, Georgia, Ghana, Greece, Hungary, Israel, Italy, Japan, Kiribati, Liechtenstein, Lithuania, Mauritius, Monaco, Morocco, Nigeria, North Macedonia, Norway, Panama, Peru, Poland, Portugal, Romania, San Marino, Sierra Leone, Slovak Republic, Spain, Sweden, Tonga, Türkiye, Ukraine, United Kingdom, USA
	Definition from another source of law	Albania, Australia, Colombia, Liechtenstein, Netherlands, Paraguay, Philippines, Serbia, Switzerland

1.4 Are there requirements with respect to notification of the exercise of powers under Article 19? If so, please provide a summary (including legislation, court decisions and practices).	Countries with any type of notification requirements [93]	Albania, Andorra, Argentina, Australia, Austria, Belgium, Bénin, Bosnia and Herzegovina, Brazil, Bulgaria, Cameroon, Canada, Chile, Costa Rica, Croatia, Czech Republic, Denmark, Dominican Republic, Estonia, Finland, France, Georgia, Germany, Greece, Iceland, Israel, Italy, Japan, Kiribati, Liechtenstein, Lithuania, Luxembourg, Monaco, Montenegro, Netherlands, North Macedonia, Norway, Panama, Paraguay, Peru, Poland, Portugal, San Marino, Senegal, Sierra Leone, Slovak Republic, Slovenia, Spain, Sri Lanka, Sweden, Switzerland, Türkiye, USA
	Countries which added additional information	Andorra, Australia, Bénin, Finland, Georgia, Netherlands, Norway, Poland, Portugal, Slovenia, Sri Lanka
2.1.1 Please summarise the legislative and other measures your country has undertaken to ensure that authorities can search or similarly access computer systems, data and data-storage mediums in your territory as described in Article 19.1. In answering, please summarise the	Court order needed[94]	Albania, Andorra, Argentina, Armenia, Australia, Azerbaijan, Belgium, Bénin, Bosnia and Herzegovina, Brazil, Bulgaria, Cabo Verde (for most cases, although the legislation provides for exceptions), Cameroon, Canada, Chile, Costa Rica, Croatia, Cyprus, Czech Republic, Denmark, Dominican Republic, Estonia, Finland, France, Georgia, Germany, Ghana, Greece, Grenada, Hungary, Iceland, Israel, Italy, Japan, Kiribati, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Mauritius, Moldova, Monaco, Montenegro, Morocco, Netherlands, Nigeria, North Macedonia, Norway, Panama, Paraguay, Peru, Philippines, Poland, Portugal, Romania, San Marino, Senegal, Serbia, Sierra Leone, Slovak Republic, Slovenia, Spain, Sri Lanka, Sweden, Switzerland, Tonga, Türkiye, Ukraine, United Kingdom, USA

[93] Most countries provided for traditional search and seizure notification. Some countries provided for special notification provisions for search and seizure of data. Given the diversity and sophistication of notification requirements readers are advised to examine countries' original answers.

[94] Throughout this matrix, a court order includes an order by a juge d'instruction or a similar judge.

requirements to be met and the procedural steps typically taken to obtain the authorisation for such a search.	No court order required	Austria, Belgium, Bénin, Canada, Colombia, Denmark, Estonia, Finland, Ghana, Greece, Hungary, Malta, Monaco, Morocco, North Macedonia, Norway, Poland, Portugal, Senegal, Slovak Republic, Sweden, Switzerland, Türkiye
2.1.2 Do particular rules apply in an emergency or other urgent circumstances? If so, please describe those rules and the applicable understanding of what constitutes an emergency.	Countries that define emergency in a text	Australia, Argentina, Austria, Azerbaijan, Bosnia and Herzegovina, Canada, Croatia, Czech Republic, Dominican Republic, Estonia, France, Georgia, Germany, Hungary, Iceland, Luxembourg, Malta, Moldova, Monaco, Morocco, North Macedonia, Norway, Poland, San Marino, Serbia, Spain, Sri Lanka, Switzerland, Ukraine, United Kingdom, USA
	Countries that rely on another source of law to handle emergencies	Albania, Andorra, Belgium, Bénin, Brazil, Bulgaria, Canada, Costa Rica, Cyprus, Denmark, Estonia, Finland, Ghana, Grenada, Israel, Japan, Lithuania, Mauritius, Nigeria, Panama, Romania, Slovenia, Tonga, Türkiye
	Countries whose authorities may act without court order in an emergency situation	Australia, Austria, Azerbaijan, Belgium, Bénin, Bosnia and Herzegovina, Brazil, Bulgaria, Cabo Verde, Canada, Chile, Croatia, Denmark, Estonia, Finland, France, Georgia, Ghana, Hungary, Italy, Lithuania, Luxembourg, Malta, Moldova, Morocco, Netherlands, North Macedonia, Norway, Poland, San Marino, Serbia, Spain, Sri Lanka, Sweden, Switzerland, Tonga, Türkiye, USA
2.1.3 Does your legislation empower your competent authorities to search or similarly access a computer system and data therein using lawfully acquired access credentials? In answering	Yes	Andorra, Armenia, Australia, Austria, Belgium, Brazil, Bulgaria, Cameroon, Canada, Costa Rica, Croatia, Cyprus, Czech Republic, Denmark, Dominican Republic, Estonia, Fiji, Finland, France, Georgia, Ghana, Greece, Grenada, Iceland, Israel, Italy, Japan, Kiribati, Liechtenstein, Luxembourg, Mauritius, Moldova, Monaco, Montenegro, Netherlands, Nigeria, North Macedonia, Mauritius, Panama, Philippines, Poland, Romania, San Marino, Senegal, Serbia, Sierra Leone, Slovenia, Switzerland,[95] Spain, Sweden, Tonga, Ukraine, USA

[95] This is pursuant not to legislation but to jurisprudence.

the question please summarise the requirements to be met and the steps typically taken to execute the power.	No	Albania, Azerbaijan, Bosnia and Herzegovina, Chile, Colombia, Hungary, Latvia, Malta, Norway, Philippines, Portugal, Slovak Republic, Sri Lanka, Türkiye, United Kingdom	
2.1.4 Does your legislation empower your competent authorities to search or similarly access a computer system and data therein using covert remote access? In answering, please summarise the requirements to be met and the steps typically taken to execute the power	No	Albania, Armenia, Austria, Azerbaijan, Bénin, Bosnia and Herzegovina (including entity of Federation of Bosnia and Herzegovina), Brazil, Bulgaria, Cabo Verde, Cameroon, Colombia, Costa Rica, Cyprus, Dominican Republic, Ghana, Grenada, Israel, Japan, Malta, Mauritius, Monaco, Panama, Portugal, Sierra Leone, Slovak Republic, Sri Lanka, Switzerland, Ukraine, United Kingdom	
	Yes	Yes (without further details)	Bosnia and Herzegovina (applicable to Entity of Republika Srpska), Italy, Liechtenstein, Luxembourg, North Macedonia, Poland, Romania, San Marino
		Available for all offences	

		Available only for certain offences	Andorra, Argentina (in some jurisdictions), Australia, Belgium, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Hungary, Iceland, Latvia, Lithuania, Moldova, Monaco, Montenegro, Netherlands, Norway, Serbia, Slovenia, Spain, Sweden, Tonga, Türkiye
		Possible in special circumstances, such as target's use of sophisticated technology	Belgium, Croatia, France, Germany, Montenegro, Spain, USA
		Court order required	Andorra, Argentina, Australia, Belgium, Brazil, Canada, Croatia, Czech Republic, Denmark, Estonia, Fiji, Finland, Georgia, Germany, Greece, Hungary, Iceland, Kiribati, Latvia, Lithuania, Moldova, Monaco, Montenegro, Netherlands, Nigeria, Norway, San Marino, Serbia, Spain, Sweden, Tonga, Türkiye, USA
		No court order required	Greece, Moldova, Senegal

			Measure includes the possibility of real time collection of data	Belgium, Denmark, Estonia, France, Georgia, Hungary, Latvia, Moldova, Monaco, Norway, Spain, Sweden, Switzerland, Tonga
			Requirements with respect to notification	Australia, Belgium, Denmark, Germany, Lithuania, Netherlands
			The measure lasts a specific period	Costa Rica, Denmark, Estonia, Finland, Germany, Israel, Netherlands, North Macedonia, Norway, Spain, Sweden
	Countries that have also attached additional information about the requirements and the execution of the measure		Australia, Belgium, Canada, Croatia, Denmark, France, Georgia, Hungary, Latvia, Lithuania, Netherlands, Serbia, Tonga	
2.1.5 Which are the competent authorities that authorise and that carry out a search as described in Article 19.1? What type of technical or other expertise is required and utilized?	Competent authorities that authorise a search	Investigating judge	Andorra, Belgium, Bénin, Cameroon, Croatia, Estonia, France, Latvia, Liechtenstein, Luxembourg, Moldova, Montenegro, Morocco, Senegal	
		Judge	Albania, Armenia, Australia, Azerbaijan, Bosnia and Herzegovina, Brazil, Bulgaria, Cabo Verde, Canada, Chile, Costa Rica, Croatia, Cyprus, Czech Republic, Denmark, Dominican Republic, Estonia, Fiji, France, Georgia, Germany, Ghana, Greece, Grenada, Hungary, Iceland, Israel, Italy, Japan, Kiribati, Lithuania, Malta, Mauritius, Monaco, Netherlands, Nigeria, North Macedonia, Norway, Peru, Philippines, Poland, Portugal, Romania, San Marino, Serbia, Sierra Leone, Slovak Republic, Slovenia, Spain, Sri Lanka, Sweden, Switzerland, Tonga, Türkiye, Ukraine, United Kingdom, USA	
		Prosecutor	Austria, Belgium, Bénin, Cameroon, Colombia, Estonia, Finland, Greece, Hungary, Luxembourg, Moldova, Monaco, Morocco, Norway, Panama, Poland, Portugal, Senegal, Slovak Republic, Sweden, Switzerland, Türkiye	

		Police officer	Belgium, Denmark, Finland, France, Ghana, Hungary, Sweden, Switzerland[96]
	Competent authorities that carry out a search	Prosecutor	Argentina, Azerbaijan, Bosnia and Herzegovina, Brazil, Cameroon, Chile, Costa Rica, France, Germany, Hungary, Italy, Japan, Lithuania, Moldova, Netherlands, North Macedonia, Norway, Panama, Peru, Poland, Portugal, Spain
		Police officer	Albania, Andorra, Argentina, Armenia, Australia, Austria, Azerbaijan, Belgium, Bénin, Bosnia and Herzegovina, Brazil, Bulgaria, Cabo Verde, Canada, Colombia, Costa Rica, Croatia, Cyprus, Czech Republic, Denmark, Dominican Republic, Fiji, Finland, France, Georgia, Germany, Ghana, Greece, Grenada, Hungary, Iceland, Israel, Italy, Japan, Kiribati, Liechtenstein, Lithuania, Luxembourg, Malta, Mauritius, Moldova, Monaco, Montenegro, Morocco, Netherlands, Nigeria, North Macedonia, Norway, Peru, Philippines, Poland, Portugal, Romania, San Marino, Senegal, Serbia, Sierra Leone, Slovenia, Spain, Sri Lanka, Sweden, Switzerland, Tonga, Türkiye, United Kingdom, USA
		Other specialised authority	Albania, Andorra, Armenia, Australia, Azerbaijan, Bénin, Bosnia and Herzegovina, Brazil, Bulgaria, Cabo Verde, Canada, Croatia, Dominican Republic, Estonia, Fiji, Finland, France, Georgia, Germany, Ghana, Greece, Grenada, Hungary, Iceland, Israel, Kiribati, Latvia, Lithuania, Mauritius, North Macedonia, Nigeria, Norway, Philippines, Poland, Portugal, Romania, San Marino, Serbia, Sierra Leone, Slovak Republic, Spain, Sri Lanka, Sweden, Switzerland, Tonga, Ukraine, United Kingdom
2.1.6 Have your authorities adopted internal standard operating procedures or	Yes		Argentina, Austria, Bosnia and Herzegovina (some institutions), Brazil, Canada, Cyprus, Czech Republic, Denmark, Dominican Republic, Estonia, Fiji, Finland, Georgia, Germany, Ghana, Greece, Grenada, Hungary, Israel,

[96] For Switzerland: only in legally provided exceptions.

similar guidelines for the search as described in Article 19.1? If possible, please provide an overview and any publicly available links.		Japan, Malta, Mauritius, Moldova, Netherlands, Nigeria, North Macedonia, Norway, Panama, Paraguay, Peru, Philippines, Poland, Romania, San Marino, Serbia, Spain, Sweden, Tonga, United Kingdom, USA	
	No	Andorra, Armenia, Australia, Azerbaijan, Belgium, Bénin, Bosnia and Herzegovina (in general), Bulgaria, Cabo Verde, Cameroon, Chile, Costa Rica, France, Iceland, Kiribati, Liechtenstein, Lithuania, Luxembourg, Monaco, Portugal, Slovak Republic, Slovenia	
2.1.7 Please provide examples of relevant court decisions related to evidence obtained by the searches as described in Article 19.1.	Cases/decisions provided	Andorra, Belgium, Bénin, Brazil, Canada, Denmark, France, Germany, Hungary, Israel, Japan, Lithuania, Luxembourg, Moldova, Nigeria, Norway, San Marino, Spain, Sweden, Switzerland, Tonga, United Kingdom, USA	
2.2.1 Please summarise what legislative or other measures have you undertaken to ensure that your authorities are able to extend the search as described in Article 19.2.	Provided in legislation	Albania, Armenia, Australia, Belgium, Bénin, Cabo Verde, Croatia, Fiji, France, Germany, Ghana, Greece, Hungary, Israel, Japan, Kiribati, Latvia, Luxembourg, Mauritius, Monaco, Montenegro, Morocco, Netherlands, Nigeria, North Macedonia, Norway, Philippines, Poland, Portugal, Romania, Senegal, Sierra Leone, Slovenia, Spain, Sri Lanka, Sweden, Tonga, Türkiye, United Kingdom, USA	
	Can obtain data from webmail	Germany, Netherlands	
	Court order required	yes	Albania, Andorra, Armenia, Azerbaijan, Belgium, Bénin, Bosnia and Herzegovina, Brazil, Bulgaria, Cabo Verde, Canada, Chile, Costa Rica, Croatia, Cyprus, Czech Republic, Denmark, Dominican Republic, Estonia, Fiji, Finland, France, Georgia, Germany, Greece, Iceland, Israel, Japan, Kiribati, Latvia, Liechtenstein, Lithuania,

			Luxembourg, Malta, Mauritius, Monaco, Montenegro, Netherlands, Nigeria, North Macedonia, Norway, Paraguay, Peru, Philippines, Poland, Romania, San Marino, Serbia, Sierra Leone, Slovak Republic, Slovenia, Spain, Sri Lanka, Tonga, Türkiye, Ukraine, United Kingdom, USA
		no	Austria, Denmark, Estonia, Ghana, Greece, Hungary, Luxembourg, Moldova, Monaco, Norway, Poland, Switzerland
2.2.2 Please summarise the procedure (including authorisations required and investigative techniques applied) for extending a search or similar accessing to another system in practice.	Country uses same procedure as for other searches	Albania, Andorra, Armenia, Australia, Austria, Azerbaijan, Belgium, Bénin, Bosnia and Herzegovina, Brazil, Bulgaria, Cabo Verde, Canada, Chile, Costa Rica, Croatia, Cyprus, Czech Republic, Denmark, Dominican Republic, Estonia, Fiji, Finland, France, Georgia, Ghana, Greece, Grenada, Hungary, Iceland, Italy, Japan, Kiribati, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Mauritius, Monaco, Montenegro,, North Macedonia, Nigeria, Norway, Panama, Paraguay, Peru, Philippines, Poland, Portugal, San Marino, Senegal, Serbia, Sierra Leone, Slovak Republic, Slovenia, Sri Lanka, Tonga, Türkiye, Ukraine, United Kingdom, USA	
	The measure is applied to data that is not in the territory of the searching country (with lawfully obtained credentials or otherwise)	Andorra, Austria, Azerbaijan, Belgium, Bénin, Brazil, Estonia, Ghana, Iceland, Luxembourg, Monaco, Netherlands, Nigeria, Poland, Senegal, Spain	
2.2.3 Please summarise how your legal framework	Defined in a text covering electronic search and seizure	Bénin, Bosnia and Herzegovina, France, Germany, Japan, Luxembourg, Montenegro, Spain, Sri Lanka, Sweden, Tonga	

applies the "grounds to believe" element of Article 19.2, including how competent authorities typically establish that they have "grounds to believe" that the data sought is stored in another computer system or part of it in its territory.	1)Requirements specified in another source of law or 2) source of requirements not stated	Albania, Andorra, Armenia, Australia, Austria, Azerbaijan, Belgium, Bosnia and Herzegovina, Brazil, Bulgaria, Cabo Verde, Canada, Chile, Costa Rica, Croatia, Czech Republic, Denmark, Dominican Republic, Estonia, Fiji, Finland, Georgia, Ghana, Greece, Hungary, Israel, Italy, Japan, Kiribati, Liechtenstein, Luxembourg, Malta, Mauritius, Monaco, Moldova, Netherlands, North Macedonia, Nigeria, Norway, Panama, Paraguay, Peru, Philippines, Poland, Portugal, Romania, San Marino, Senegal, Serbia, Sierra Leone, Slovak Republic, Slovenia, Switzerland, Türkiye, United Kingdom, USA
2.2.4 Please summarise how your legal framework applies the "in its territory" element of Article 19.2, including whether or not your framework imposes an affirmative requirement that the connected system be in your territory.	Framework imposes an affirmative requirement that the connected system be in the territory of the country executing the measure	Armenia, Bosnia and Herzegovina (including entity of Federation of Bosnia and Herzegovina), Bulgaria, Canada, Costa Rica, Greece, Grenada, Kiribati, Latvia, Mauritius, North Macedonia, Paraguay, Philippines, San Marino, Tonga, USA
	Framework does not impose an affirmative requirement that the connected system be in the country executing the measure	Albania, Andorra, Australia, Austria, Azerbaijan, Belgium, Bénin, Bosnia and Herzegovina (applicable to entity of Republika Srpska and Brcko District), Brazil, Cabo Verde, Chile, Croatia, Czech Republic, Denmark, Dominican Republic, Estonia, Fiji, Finland, France, Georgia, Germany, Ghana, Hungary, Iceland, Israel, Italy, Japan, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Moldova, Monaco, Montenegro, Netherlands, Nigeria, Norway, Peru. Poland, Portugal, Senegal, Serbia, Sierra Leone, Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Türkiye, Ukraine, United Kingdom, USA
2.2.5 How do you proceed in cases when it cannot be determined where the data sought is stored ("loss of (knowledge of) location situations")?	Country continues as if the data is in its territory	Australia, Austria, Bénin, Bosnia and Herzegovina, Brazil, Croatia, Czech Republic, Denmark, Dominican Republic, Estonia, France, Germany, Greece, Hungary, Italy, Luxembourg, Moldova, Monaco, Netherlands, Nigeria, Philippines, Poland, Portugal, Senegal, Serbia, Slovenia, Spain, Switzerland, Türkiye
	Country stops pursuing this data	Canada, Chile, Costa Rica, Grenada, Kiribati, Paraguay, Peru, San Marino, Sierra Leone, Slovak Republic

	Decided case by case	Andorra, Belgium, Bulgaria, Finland, Ghana, Israel, Japan, Latvia, Mauritius, Norway, San Marino, Sri Lanka, Sweden, United Kingdom, USA
2.2.6 Please provide typical examples (use cases) for extending a search.	Cases/decisions provided	Andorra, Armenia, Austria, Belgium, Bénin, Bosnia and Herzegovina, Brazil, Bulgaria, Czech Republic, Estonia, France, Germany, Ghana, Hungary, Iceland, Japan, Liechtenstein, Lithuania, Luxembourg, Netherlands, Norway, Paraguay, Peru, Poland, Portugal, Serbia, Slovak Republic, Slovenia, Spain, Sweden, Tonga, Türkiye, USA
2.2.7 Please provide examples of relevant court decisions related to the extension of a search to a connected computer system.	Cases/decisions provided	Belgium, Bénin, Brazil, France, Germany, Hungary, Israel, Lithuania, North Macedonia, Norway, Sweden, Switzerland
2.3.1 Please summarise what legislative or other measures your country has undertaken to ensure that your authorities are able to seize or similarly secure computer data as described in Article 19.3. In answering, please summarise the requirements to be met and the procedural steps typically taken to obtain the authorisation for such a seizure.	Countries with specific elements of Art. 19.3 in a specific text	Albania, Argentina, Armenia, Austria, Belgium, Bénin, Bosnia and Herzegovina (entity of Federation of Bosnia and Herzegovina), Bulgaria, Cabo Verde, Cameroon, Croatia, Czech Republic, Dominican Republic, Fiji, Finland, France, Georgia, Germany, Ghana, Greece, Grenada, Hungary, Israel, Italy, Japan, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Mauritius, Monaco, Montenegro, Netherlands, Nigeria, North Macedonia, Panama, Philippines, Poland, Portugal, Senegal, Sierra Leone, Slovak Republic, Spain, Sri Lanka, Sweden, Switzerland, Tonga, United Kingdom
	Countries that rely on another source of law to apply the elements of Art. 19.3	Andorra, Azerbaijan, Belgium, Bosnia and Herzegovina (applicable to Brcko District), Cameroon, Chile, Costa Rica, Brazil, Cyprus, Denmark, Estonia, Germany, Ghana, Israel, Liechtenstein, Lithuania, Malta, Moldova, Morocco, Nigeria, Norway, Peru, Paraguay, San Marino, Serbia, Slovenia, Sweden, Switzerland, Ukraine, USA

	Countries that cannot apply the elements of Art. 19.3		Bosnia and Herzegovina (including entity of Republika Srpska), Bulgaria, Canada, Denmark, Estonia, Georgia, Ghana, Kiribati, Malta, Moldova, Nigeria, North Macedonia, Poland, Romania, Sweden, Switzerland, Türkiye
2.3.2 Do you apply the same measures when extending a search (according to Article 19.2) and in situations when it cannot be determined where the data sought is stored?	Yes		Albania, Andorra, Armenia, Australia, Belgium, Bénin, Bosnia and Herzegovina, Bulgaria, Cabo Verde, Canada, Chile, Costa Rica, Croatia, Czech Republic, Denmark, Dominican Republic, Estonia, Fiji, Finland, France, Germany, Ghana, Greece, Hungary, Israel, Italy, Japan, Liechtenstein, Lithuania, Luxembourg, Malta, Mauritius, Moldova, Monaco, Netherlands, Nigeria, North Macedonia, Nigeria, Norway, Panama, Peru, Philippines, Poland, Senegal, Serbia, Sierra Leone, Slovenia, Spain, Sri Lanka, Sweden, Switzerland, Tonga, Türkiye, United Kingdom, USA
	No		Kiribati, Grenada
2.3.3 Which are the competent authorities that authorise and that carry out a seizure as described in Article 19.3? What type of technical or other expertise is required and utilized?	Authorities that authorise a seizure	Judge	Albania, Argentina, Armenia, Australia, Azerbaijan, Bosnia and Herzegovina, Brazil, Bulgaria, Cabo Verde, Canada, Chile, Colombia, Costa Rica, Croatia, Cyprus, Czech Republic, Denmark, Dominican Republic, Estonia, Fiji, Finland, France, Georgia, Germany, Ghana, Greece, Grenada, Hungary, Iceland, Israel, Italy, Japan, Kiribati, Lithuania, Malta, Mauritius, Monaco, Montenegro, Netherlands, Nigeria, North Macedonia, Norway, Panama, Paraguay, Peru, Philippines, Poland, Romania, San Marino, Serbia, Sierra Leone, Slovak Republic, Slovenia, Spain, Sri Lanka, Sweden, Switzerland, Tonga, Türkiye, Ukraine, United Kingdom, USA
		Investigative judge	Andorra, Belgium, Bénin, Cameroon, Croatia, Estonia, France, Latvia, Liechtenstein, Luxembourg, Moldova, Morocco, Senegal[97]

[97] Senegal: a juge d'instruction may also execute the search.

		Prosecutor	Austria, Belgium, Bénin, Cameroon, Chile, Estonia, Finland, Greece, Hungary, Luxembourg, Moldova, Monaco, Morocco, Netherlands, Norway, Poland, Portugal, Senegal, Slovak Republic, Sweden, Switzerland, Türkiye
		Police officer	Belgium, Finland, France, Ghana, Hungary, Iceland, Norway, Sweden
	Authorities that carry out a seizure	Prosecutor	Argentina, Azerbaijan, Bosnia and Herzegovina, Brazil, Cameroon, Costa Rica, Dominican Republic, Germany, Hungary, Italy, Japan, Lithuania, Moldova, Netherlands, North Macedonia, Norway, Panama, Paraguay, Peru, Poland, Romania, Spain
		Police officer	Albania, Andorra, Argentina, Armenia, Australia, Austria, Azerbaijan, Belgium, Bénin, Bosnia and Herzegovina, Brazil, Bulgaria, Cabo Verde, Cameroon, Canada, Colombia, Costa Rica, Croatia, Cyprus, Czech Republic, Denmark, Dominican Republic, Fiji, Finland, France, Georgia, Germany, Ghana, Greece, Hungary, Iceland, Israel, Italy Japan, Kiribati, Liechtenstein, Lithuania, Luxembourg, Malta, Mauritius, Moldova, Monaco, Montenegro, Netherlands, Nigeria, North Macedonia, Norway, Peru, Philippines, Poland, Portugal, Romania, San Marino, Senegal, Serbia, Sierra Leone, Slovenia, Spain, Sri Lanka, Sweden, Switzerland, Tonga, Türkiye, United Kingdom, USA
		Other specialised authority	Albania, Andorra, Armenia, Australia, Azerbaijan, Bénin, Bosnia and Herzegovina, Brazil, Bulgaria, Cabo Verde, Canada, Costa Rica, Croatia, Denmark, Dominican Republic, Estonia, Fiji, Finland, France, Georgia, Ghana, Greece, Grenada, Hungary, Israel, Kiribati, Lithuania, Malta, Mauritius, Montenegro, Nigeria, North Macedonia, Norway, Philippines, Poland, San Marino, Serbia, Sierra Leone, Slovak Republic, Spain, Sri Lanka, Sweden, Switzerland, Tonga, Türkiye, United Kingdom

2.3.4 Please provide typical examples (use cases) and relevant court decisions.	Cases/decisions provided	Andorra, Armenia, Belgium, Bénin, Bosnia and Herzegovina, Brazil, Czech Republic, France, Germany, Hungary, Japan, Lithuania, Luxembourg, Mauritius, North Macedonia, Peru, Switzerland, Tonga, Türkiye, USA
2.4.1 Please summarise what legislative or other measures your country has undertaken to ensure that your authorities are able to order a person to provide necessary information as described in Article 19.4. Please summarise the rules applicable to this provision.	Defined in a text covering electronic search and seizure	Albania, Andorra, Armenia, Australia, Austria, Belgium, Bosnia and Herzegovina (applicable to entities of Federation Bosnia and Herzegovina, Republika Srpska and Brcko District), Cabo Verde, Canada, Croatia, Dominican Republic, Fiji, Georgia, Ghana, Grenada, Hungary, Japan, Kiribati, Liechtenstein, Luxembourg, Mauritius, Monaco, Morocco, Netherlands, North Macedonia, Norway, Philippines, Portugal, Senegal, Serbia, Sierra Leone, Slovak Republic, Slovenia, Spain, Sri Lanka, Sweden, Switzerland, Tonga, United Kingdom, USA
	Derived from another source of law	Austria, Azerbaijan, Bénin, Bosnia and Herzegovina, Brazil, Bulgaria, Canada, Costa Rica, Cyprus, Czech Republic, Denmark, Estonia, Finland, Georgia, Germany, Ghana, Hungary, Iceland, Israel, Italy, Liechtenstein, Lithuania, Malta, Moldova, Montenegro, Nigeria, North Macedonia, Panama, Poland, Portugal, Peru, Paraguay, San Marino, Serbia, Sweden, Switzerland, USA
2.4.2 Please provide typical examples (use cases) and relevant court decisions.	Cases/decisions provided	Andorra, Belgium, Bénin, Brazil, Czech Republic, France, Germany, Hungary, Israel, Japan, Lithuania, Luxembourg, Peru, Norway, Slovenia, USA
3.1.1 Please summarise the conditions and safeguards that are applicable when applying the different measures for the search, extension of the search, and seizure of	Almost every country reported that it included human rights safeguards and protections when implementing Article 19. However, countries' responses to this question were so numerous and diverse that it was impossible to reflect them in the matrix - some countries gave general answers, adverting to treaty and constitutional obligations; other countries provided lengthy specific lists of	

stored computer data described above.	available remedies (and no two lists were identical). For these reasons, only the assessment contains a (brief) discussion of each country's approach to human rights protections and safeguards vis-a-vis Article 19. Readers interested in countries' answers to this question should consult the compilation, where those answers appear	