UNODC
United Nations Office on Drugs and Crime

# Electronic Evidence Country Fiche: INDIA

## 1) DEFINITIONS

| India |
|---|
| **What are the definitions in your laws/regulations, if any, of:** |
| **Electronic evidence** |
| Although there is no specific definition of “electronic evidence”, Indian legislation provides the concept of "electronic evidence" through the Information Technology Act, 2000 ("IT Act") and the related amendments in the Evidence Act, 1872 ("Evidence Act") and the Indian Penal Code, 1860 ("IPC"). It is an Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as “electronic commerce”, which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies. Even if the term electronic evidence not explicitly defined, according to Section 2(1)(t) of the IT Act (as amended in 2008), the term "electronic record" means data, record or data generated, image or sound stored, received or sent in an electronic form or micro-film or computer-generated micro fiche. Section 4 of the IT Act expressly recognises the validity and use of electronic records in place of ordinary paper-based records. |
| **Computer system** |
| The Information Technology Act, 2000, Section 2(1) defines the source of electronic data. Specifically, “computer system” means a device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files, which contain computer programmes, electronic instructions, input data and output data, that performs logic, arithmetic, data storage and retrieval, communication control and other functions (Section 2 (1)(l)).<br>Additionally, “computer network” means the inter-connection of one or more computers or computer systems or communication device through– (i) the use of satellite, microwave, terrestrial line, wire, wireless or other communication media; and (ii) terminals or a complex consisting of two or more interconnected computers or communication device whether or not the inter-connection is continuously maintained |

| |
|---|
| (Section 2(1)(j)[1]). "Computer resource" includes computer, computer system, computer network, data, computer data base or software (Section 2(1)(k)). |
| **Computer data** |
| The term "computer data" does not seem to be explicitly defined. However, the Information Technology Act, 2000, Section 2(1) establishes that "computer" means any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software or communication facilities which are connected or related to the computer in a computer system or computer network (Section 2(1)(i)). According to art. 2(1)(o) of the same provision, "data" means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer. |
| **Categories of computer data (e.g. basic subscriber information, traffic data and content data)** |
| India's legislation provides partial definitions of the specific types of data.<br>According to art. 69B (ii) "traffic data" means any data identifying or purporting to identify any person, computer system or computer network or location to or from which the communication is or may be transmitted and includes communications origin, destination, route, time, data, size, duration or type of underlying service and any other information.<br>While "subscriber" means a person in whose name the [electronic signature][2] Certificate is issued (Section 2 (1) (zg)).<br><br>The term "content data" does not appear to be explicitly defined. |
| **Electronic surveillance or real-time collection of computer/communication data** |
| Although a specific definition of the term "electronic surveillance" does not appear to be available, there are several provisions giving a framework to it. The Indian Telegraph Act, 1885; Information Technology Act, 2000 (as amended 2008); The IT (Procedures and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009; |

[1] Subs. by s. 4, ibid., for clause (j) (w.e.f. 27-10-2009).
[2] Subs. by Act 10 of 2009, s. 2, for —digital signature‖ (w.e.f. 27-10-2009).

| |
|---|
| Section 3 (1)(j) of the Information Technology (Intermediary Guidelines) Rules, 2021 in reformulating Section 3(7) of the 2011 Rules. |
| **Service provider (e.g. ISP, hosting)** |
| The term service provider is described through the term intermediary under Section 2 (1), of the the Information Technology Act, 2000. It provides that 'with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes' |

## 2) DATA RETENTION REGIME

| |
|---|
| India |
| **Do you have any domestic laws that stipulate a mandatory retention period of electronic data? If so, for what types of data and for how long?** |
| Section 67C Preservation and Retention of information by intermediaries (1): Intermediary shall preserve and retain such information as may be specified for such duration and in such manner and format as the Central Government may prescribe.<br>Data Retention/Preservation: The G-8 24/7 Network for data preservation is one of the channels to get the data preserved expeditiously.<br>Generally, the data is preserved for an initial period of 90 days from the receipt of Request. During this period, the investigation Agencies including State Law Enforcement Agencies should send a proposal to IS-II Division, MHA for issue of LR or MLA Request for obtaining the data from concerned service provider. If the investigation continues, then after every additional 60 days the request for preservation of data shall be served to the country concerned. |

## 3) ADMISSIBILITY OF ELECTRONIC EVIDENCE IN THE CRIMINAL TRIAL

| |
|---|
| India |

UNODC
United Nations Office on Drugs and Crime

| **What is the requirement under your domestic law for electronic evidence to be admissible in criminal trial?** |
| --- |
| Section 4 of the 1872 Evidence Act (last updated 2020) establishes the criteria for the legal recognition of electronic records, providing that:<br>Where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is:<br>(a) rendered or made available in an electronic form; and<br>(b) accessible so as to be usable for a subsequent reference.<br>Section 65A of the Evidence Act provides that the contents of electronic records may be proved in accordance with the provisions of Section 65B of the Evidence Act. Thus, any documentary evidence by way of an electronic record can be proved only in accordance with the procedure prescribed under Section 65B of the Evidence Act. Section 65B of the Evidence Act provides that notwithstanding anything contained in the Evidence Act, any information contained in an electronic record, whether it be the contents of a document or communication printed on a paper, or stored, recorded, copied in optical or magnetic media produced by a computer, it is deemed to be a document and is admissible in evidence without further proof of the production of the original, subject to satisfaction of the conditions set out in Section 65B(2) - (5) of the Evidence Act.<br>Section 65B of the Evidence Act provides for both technical conditions and non-technical grounds for admissibility of electronic evidence. Sub-section (2) of Section 65B of the Evidence Act lists the technological conditions upon which a duplicate copy (including a print-out) of an original electronic record may be used. These are:<br>a) At the time of the creation of the electronic record, the computer that produced it must have been in regular use;<br>b) The kind of information contained in the electronic record must have been regularly and ordinarily fed in to the computer;<br>c) The computer was operating properly; and<br>d) The duplicate copy must be a reproduction of the original electronic record.<br><br>As can be inferred the above conditions relate to veracity of the data. The conditions have a twofold impact as they i) ensure that there has been no unauthorised use of the data; and ii) the device was functioning properly, ensuring accuracy and genuineness of the reproduced data.<br>In any proceedings where it is desired to give a statement in evidence by virtue of this section, a certificate that is:<br>(a) identifying the electronic record containing the statement and describing the manner in which it was produced; |

(b) giving such particulars of any device involved in the production of that electronic record as may be appropriate for the purpose of showing that the electronic record was produced by a computer;

(c) dealing with any of the matters to which the conditions mentioned above relate, and purporting to be signed by a person occupying a responsible official position in relation to the operation of the relevant device or the management of the relevant activities, shall be evidence of any matter stated in the certificate; and it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it.

Sub-section (3) of Section 65B of the Evidence Act is self-explanatory and confirms that if the user has been using a networked device either to store or process information, all the connected devices will be considered to be a single device.

Provisions of the Indian Evidence Act, 1872 on admissibility of electronic evidence (as amended):

- Amendment to Section 17 so that the definition of the term admission will include statements in electronic form also;
- Addition of Section 22A to make oral admission of the contents of an electronic record ire levant unless the genuineness of the record is in question;
- Addition of Section 39 to provide that the court can decide the part of the electronic record is to be submitted to fully understand the nature and effect of the evidence and the circumstances under which it was made.
- Addition of Sections 81A, 85A, 85B, 85C, 88A and 90A to provide a presumption of authenticity to certain electronic records like official gazettes, digital signatures, electronic messages etc.
- The law as it stands today provides for the production of information in digital form as evidence in a court of law without the additional burden of producing them in tangible form and proving the authenticity of such copies.

## 4) RECEIVING REQUESTS FOR ELECTRONIC EVIDENCE FROM OTHER STATES

### 4.1. **Direct requests** from foreign authorities to service providers

#### *4.1.1. Requests for preservation*

| India |
| --- |
| **What legal framework(s) is/are applicable, if any?** |

| |
|---|
| Indian legislation does not provide an explicit ruling on whether it is possible to send requests directly to service provider based in the country. |
| **Are the service providers in your country prohibited from or have limited capacity for executing such requests from foreign authorities?** |
| Information not officially provided. |
| **If they are prohibited or if there are limitations, are there any alternative options to preserve the data from your country, e.g. through police-to-police cooperation, specialized networks (e.g. G7/8 24/7 Network) or mutual legal assistance (MLA)?** |
| <u>International treaties:</u><br>- 2000 United Nations Convention against Transnational Organized Crime (Palermo Convention) art. 18(4) and (5);<br>- The United Nations Convention Against Corruption (2003) art. 43 and 46;<br>- United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substance, 1988 (Vienna Convention)<br>- Hague Convention<br>- SAARC Convention<br><br><u>For Commonwealth States:</u><br>- The Revised Harare Scheme 2011: The Commonwealth States have adopted alternate schemes for international cooperation based on domestic legislation rather than treaties, and these arrangements have been consolidated into the Scheme Relating to Mutual Assistance in Criminal Matters within the Commonwealth (the Harare Scheme).<br>The Harare Scheme is not a legally binding instrument or treaty, per se. It is a voluntary arrangement, which Commonwealth States are expected to implement through domestic legislation.<br>Paragraphs: 1(5)(j) allows for obtaining electronic evidence; 21(7) provides for electronic evidence; 24 provides for real-time collection of traffic data; and 23 provides for real-time collection of content.<br><br><u>Bilateral treaties</u>:<br>For countries who have not ratified nor implemented the above-mentioned instruments, to provide international cooperation and assistance The Mutual Legal Assistance Treaties (MLATs) in criminal matters are applicable, as bilateral treaties. India has |

entered into Mutual Legal Assistance Treaties/Agreements with 42 countries (November 2019).
India provides mutual legal assistance in criminal matters through Bilateral Treaties/Agreements, Multilateral Treaties/Agreements or International Conventions or on the basis of assurance of reciprocity.
The Government of India Ministry of Home Affairs IS-II Division/Legal Cell-I issued the Comprehensive Guidelines for investigation abroad and issue of Letters Rogatory (LRs)/ Mutual Legal Assistance (MLA) Request and Service of Summons/Notices/Judicial documents in respect of Criminal Matters F. No. 25016/52/2019-LC setting common grounds for the different measures applicable in the context of international judicial cooperation regulated by MLATs.

In India the following instruments shall be used to gather electronic evidence cross-border: Mutual legal Assistance Request; Letters Rogatory; Service of Summon, Notices and Judicial Processes.

Letter of Rogatory (LR) is issued by the Indian Court on the request of the Investigating Officer or Investigating Agency under Section 166A and Chapter VII A of CrPC. LRs can be issued to the countries with whom India has Bilateral Treaty/Agreement, Multilateral Treaty/Agreement or International Convention under the same arrangements.
Further, LR can also be issued to any other country (with whom India does not have any existing Bilateral Treaty/Agreement, Multilateral Treaty/Agreement or International Convention) on the basis of assurance of Reciprocity.

<u>Police-to-Police cooperation:</u>
India as member state of Interpol, hosts an INTERPOL National Central Bureau (NCB). This connects their national law enforcement with other countries and with the General Secretariat via the Interpol secure global police communications network called I-24/7. For getting informal information or leads, the assistance can be sought through INTERPOL Channels. The Investigating Agency is required to take up the matter with Assistant Director, NCB, Central Bureau of Investigation, 5-B, CGO Complex, Lodhi Road, Jawaharlal Nehru Stadium Marg, New Delhi-110003.

Additionally, spontaneous information can be shared according to Art. 18 (4) and (5) of the United Nations Convention against Transnational Organized Crime, which specifies the type of MLA that can be requested including, among others, “taking evidence…”, “providing evidentiary items…”, “executing searches and seizures…”, and “other type of assistance not contrary to the domestic law of the requested State”.

**Is a judicial order required from the requesting state?**

| |
|---|
| For an incoming request, it does not seem to be explicitly required by the law. |
| **Are there any time limits for data preservation? Any possibility of extension?** |
| It does not seem to be explicitly indicated by the law |
| **Would service providers in your country notify the data subjects of the request?** |
| Information not officially provided. |

*4.1.2. Requests for voluntary disclosure*

| India |
|---|
| **What legal framework(s) is/are applicable, if any?** |
| Any specific rule is indicated in the Indian legislation related to voluntary disclosure. |
| **Are the service providers in your country prohibited from or have limited capacity for executing such requests from foreign authorities?** |
| Information not officially provided. |
| **If they are prohibited or if there are limitations, are there any alternative options to preserve the data from your country, e.g. through police-to-police cooperation, specialized networks (e.g. G7/8 24/7 Network) or mutual legal assistance (MLA)?** |
| No specific rule related to voluntary disclosure or alternative methods to MLA. In addition, there are no rules indicating the value of evidence procured in such ways. However, foreign authorities may consider requesting assistance through the police-to-police cooperation channel, Interpol I-24/7, G7 24/7 or via MLA, or a spontaneous information sharing is always granted also under Art. 18 (4) and (5) of the United Nations Convention against Transnational Organized Crime (as indicated above). |
| **Is a judicial order required from the requesting state? Are there any time limits?** |
| Information not officially provided. |
| **Would service providers in your country notify the data subjects of the request?** |

| |
|---|
| Information not officially provided. |
| **How can the process be simplified or quickened in emergency situations?** |
| In urgent circumstances, a request may be made orally or by email or facsimile or any other agreed forms of electronic media or through INTERPOL but shall be confirmed in writing by the Investigating Agency or State Government/UT concerned with all relevant documents within 5 days after making such request to IS-II Division, MHA. |

4.2. Requests received by your central authority for **Mutual Legal Assistance (MLA)**

| India |
|---|
| **How do you execute MLA requests for electronic evidence stored by domestic service providers (e.g. through a domestic court order or a search warrant)?** |
| The MLA request is executed through the Indian Central Authority. According to the Comprehensive Guidelines for investigation abroad and issue of Letters Rogatory (LRs)/ Mutual Legal Assistance (MLA) Request and Service of Summons/Notices/Judicial documents in respect of Criminal Matters F. No. 25016/52/2019-LC there are specific procedure indicated for outgoing and incoming requests.<br><br>Incoming request<br>Section 166B, Section 105K and Chapter VII A of CrPC[3], Section 58 and Section 61 of PMLA[4], gives the outline of execution of an incoming request in India. All the requests to India for the mutual legal assistance in criminal matters are made to the Central Authority of India. The requests received through diplomatic channels by Ministry of External Affairs i.e. Territorial Division, CPV Division, etc., are also forwarded to IS-II Division, MHA (Central Authority).<br>All incoming requests are received by Central Authority of India. The Central Authority of India examines the incoming request on the following grounds:<br>a) On the basis of provisions of MLAT or other Bilateral Treaties/Agreements, Multilateral Treaties/Agreements or International Conventions if exists with the requested country or assurance of reciprocity.<br>b) Whether the request made is of Civil or Criminal nature. |

[3] Criminal procedural code

[4] Prevention of money laundering Act

c) Whether the request infringes or is specifically barred by any domestic law in India.

The procedure and the related articles are indicated in the MLA section below.

**Can you provide assistance in real-time collection of non-content and/or content data (e.g. through electronic surveillance) upon the receipt of a MLA request? If yes, are there any limitations or conditions (e.g. limited to certain crime types or penalties thresholds)?**

As per Indian law, surveillance is prohibited, nevertheless, surveillance conducted by the Government is legal if a proper legal channel is followed by the appropriate Government. In the legal regime of technology, the concerned laws governing communication surveillance in India, are:

1. The Indian Telegraph Act, 1885, which majorly deals with the interception of calls by the government.
   The Government derives its right of interception from Section 5 of The India Telegraph Act, which grants power for Government to take possession of licensed telegraphs and to order interception of messages". Section 5(2) of the Act contains the criteria due to which the central or state government authority has power over the transmission, interception, and retention of any communication
2. Indian Information Technology Act, 2000. The statute primarily addresses data interception, which means it governs digital surveillance. According to Section 69 of the Information Technology Act, "power to issue directions for interception or monitoring or decryption of any information through any computer resource". This provision vests authority in either the central or the state governments "to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted, received or stored in any computer resource". Section 69 of the IT Act is more extensive in this regard. Surveillance can now be carried out by the appropriate authority even for the investigation of any offence.
   According to the Information Technology Act, 2000 (as amended 2008) the service provided (defined by the term 'intermediary') shall provide the assistance and extend all facilities to enable online access to the requesting agency to the computer resource to generate, transmit, receive, monitor collect or store traffic data or information.
   Section 29 establishes that the Controller, or any person authorized by him, shall have access to any computer system, any apparatus, data or any other material connected with such system, for the purpose of searching or causing a search to be made for obtaining any information or data contained in or available to such computer system if he has reasonable cause to suspect that any contravention

of the provisions of this chapter made there under has been committed. For these purposes the Controller, or any person authorized by him may, by order, direct any person in charge of, or otherwise concerned with the operation of the computer system, data apparatus or material, to provide him with such reasonable technical and other assistant as he may consider necessary.

Section 69B establishes the power to authorise to monitor and collect traffic data or information through any computer resource for cyber security. (1) The Central Government may, to enhance cyber security and for identification, analysis and prevention of intrusion or spread of computer contaminant in the country, by notification in the Official Gazette, authorise any agency of the Government to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource. (2) The intermediary or any person in-charge or the computer resource shall, when called upon by the agency which has been authorised under sub-section (1), provide technical assistance and extend all facilities to such agency to enable online access or to secure and provide online access to the computer resource generating, transmitting, receiving or storing such traffic data or information […].

In 2018 government has ordered under Rule 4 provides that "the competent authority may authorize an agency of the Government to intercept, monitor or decrypt information generated, transmitted, received or stored in any computer resource for the purpose specified in sub-section (1) of Section 69 of the Act".

3. The Information Technology Rules are also in place in India for the procedural governance of surveillance. The IT (Procedures and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009, majorly deals with the procedural requirements. The IT Rule, 2009, specifies the comprehensive method and safeguards for the interception of information, including safeguards such as recording the grounds for interception and the directives for the interception shall not exceed beyond the period of 60 days, it can be further extended up to 180 days, not beyond that, destruction of information or record so obtained through interception within 6 months, etc.

Limitation: the collaboration of the intermediaries is required under the Information Technology Act, 2000 to enhance cyber security and for identification, analysis and prevention of intrusion or spread of computer contaminant in the country, by notification in the Official Gazette.

Section 3 (1)(j) of the Information Technology (Intermediary Guidelines) Rules, 2021 in reformulating Section 3(7) of the 2011 Rules, claims that when required by lawful order, the intermediary shall provide information or any such assistance to Government Agencies who are lawfully authorised for investigative, protective, cyber security activity. The information or any such assistance shall be provided for the purpose of

verification of identity, or for prevention, detection, investigation, prosecution, cyber security incidents and punishment of offences under any law for the time being in force, on a request in writing staling clearly the purpose of seeking such information or any such assistance.

**What are the central and competent authorities in your country to:**

**a) Receive a request for MLA in criminal matters?**

**b) Execute/recognize the measure (if other than the receiving authority)?**

The competent authority to receive the requests/decisions for judicial cooperation is the Ministry of Home Affairs, Internal Security-II Division is the Central Authority of India for dealing with requests of mutual legal assistance in criminal matters.

The competent authority to execute the requests/decisions for judicial cooperation is the Ministry of Home Affairs, Internal Security-II Division is the competent authority to execute the requests/decisions for judicial cooperation. It receives requests from foreign countries and promptly gets the requests executed through the appropriate Authority, in accordance with the Indian laws and in the manner specified by the foreign country, if it is not contrary to Indian law.

*Note:*

The Central Authority of India i.e., Ministry of Home Affairs performs the following functions with respect to providing and obtaining mutual legal assistance in criminal matters: i) It ensures that the widest measure of legal assistance is provided by India ii) It formulates and takes the policy decision on mutual legal assistance in criminal matters. iii) It reviews all requests received by it from the Investigating Agencies/State Governments/UTs/Judicial Authorities and takes appropriate actions. If necessary, it corresponds with the agency or Court sending the request regarding the inadequacy or the need to supplement a request and provide information on how they can be improved. iv) For delivering the request to foreign country and follow up of the requests, the IS-II Division, MHA functions through AD (IPCC), CBI. v) It receives requests from foreign countries. vi) It promptly gets the requests executed through the appropriate Authority, in accordance with the Indian laws and in the manner specified by the foreign country, if it is not contrary to Indian law. vii) It answers queries related to Indian law and provides information to the countries wishing to make requests to India viii) It coordinates arrangements for the representation of foreign countries in India for any proceedings arising out of a request for assistance. ix) It periodically participates in the bilateral consultations with the Central Authority of the Contracting States to take measure for the prevention and suppression of crime and early execution of requests. x) It arranges training for Indian law enforcement agencies in coordination with CPV Division MEA, AD (IPCC) CBI, NIA and State Police Authorities. It takes assistance of

AD (IPCC), CBI for arranging the training programmes at CBI academy or at State Police academies. xi) It arranges training programmes in coordination with foreign experts on the subject of mutual legal assistance in criminal matters and extradition.

**What are the accepted languages for MLA requests?**

The request for assistance and all the supporting documents shall be provided in English and wherever necessary, the request and the supporting documents should be translated into the language required by the Requested Country. The translated copies (if any) should be duly certified by the translator and authenticated by the concerned Investigating Agency.

**Can the request be submitted electronically to the central authority?**

Yes, it can be submitted electronically. In general, it can be transmitted by:

- Courier or post
- Fax
- Email: Yes
- Diplomatic channels
- Liaison Officers
- Interpol
- Direct communication between authorities

Courier/postal mail, Email, Fax: In urgent cases but the same is to be following through proper channel within 15 to 30 days of such request.

Telephone: 91 11 230 92 785
Fax: 91 11 230 93 155
Email: js-is2@mha.gov.in
Website: www.mha.gov.in

In urgent cases the same is to be following through proper channel within 15 to 30 days of such request.

Contact person
Name: Shri Anoop Yadav
Position: Deputy Legal Advisor
Telephone: 001 230 75 116
Email: anoop.yadav@gov.in

Office time 9.00 to 17.30.

| **Can the request be submitted directly to the central authority?** |
| --- |
| Yes, the Central Authority transmits and receives all requests for assistance either directly or through diplomatic channels.<br><br>Address:<br>Ministry of Home Affairs<br>North Block<br>New Delhi<br>110 001 |
| **What are the specific requirements (e.g. dual criminality, minimum penalty thresholds, etc.) that the requesting states have to meet under your domestic laws for MLA requests seeking for the provision of electronic evidence?** |
| India provides mutual legal assistance in criminal matters through Bilateral Treaties/Agreements, Multilateral Treaties/Agreements or International Conventions or on the basis of assurance of reciprocity.<br>The request for assistance is generally refused if:<br>i) the execution of the request would impair sovereignty, security, public order and essential public interest of India or foreign country.<br>ii) the request for assistance has been made for the purpose of investigating and prosecuting a person on account of that person's sex, race, religion, nationality, origin or political opinions or that person's position may be prejudiced for any of those reasons.<br>iii) the request is made for conduct or offence which is an offence under military law but not an offence under ordinary criminal law in India or foreign country.<br>iv) the request relates to an offence in respect of which the accused person has been finally acquitted or pardoned.<br>v) *de minimis* request is made i.e. the request is trivial or disproportionate in nature.<br>vi) the request seeking restraint, forfeiture or confiscation of proceeds and instrumentalities of crime or seizure of property is in respect of conduct/activity which cannot be made the basis for such restraint, forfeiture, confiscation or seizure in the Contracting States.<br>The execution of request may be postponed if it would interfere with an ongoing criminal investigation, prosecution or proceeding in the Contracting States. Such request may be executed subject to conditions determined necessary after consultations with the Central Authority of the Requesting Country. |

## 5) REQUESTING ELECTRONIC EVIDENCE ACROSS BORDERS

5.1. **Direct requests** to foreign service providers

*5.1.1. Requests for preservation*

| India |
| --- |
| **What legal framework(s) is/are applicable, if any?** |
| The request for data protection/preservation may be sent using official ID's directly to the service provider or through the Assistant Director (NCB), Central Bureau of Investigation, 5-B, 6th Floor, CGO Complex, Lodhi Road, Jawaharlal Nehru Stadium Marg, New Delhi-110003 ((email: adipol@cbi.gov.in and Telefax:011-24364070), who would in turn get the data preserved through Cyber Crime Investigation Cell (EOU-IX) of CBI which is being the contact point in respect of India G-8 24/7 Network. It allows Law Enforcement Agencies of India making urgent preservation requests of the digital data before it perishes. CBI will keep the Central Authority of India informed of such preservation requests. |
| **Which authority(ies) in your country is/are allowed to request data preservation to foreign service providers?** |
| Cyber Crime Investigation Cell (EOU-IX) of CBI which is being the contact point in respect of India G-8 24/7 Network. |
| **If the requested foreign service providers are prohibited or limited to preserve the data, are there any alternative options to preserve the data, e.g. through police-to-police cooperation, specialized networks (e.g. G7/8 24/7 Network) or MLA?** |
| Police-To-police cooperation: INTERPOL National Central Bureau (NCB). This connects their national law enforcement with other countries and with the General Secretariat via the Interpol secure global police communications network called I-24/7. For getting informal information or leads, the assistance can be sought through INTERPOL Channels. The Investigating Agency is required to take up the matter with Assistant Director, NCB, Central Bureau of Investigation, 5-B, CGO Complex, Lodhi Road, Jawaharlal Nehru Stadium Marg, New Delhi-110003.<br><br>Cooperation under the international legal framework (2000 United Nations Convention against Transnational Organized Crime (Palermo Convention) art. 18(4) and (5); The United Nations Convention Against Corruption (2003) art. 43 and 46; United Nations |

Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substance, 1988 (Vienna Convention); Hague Convention; SAARC Convention)

Mutual Legal Assistance. Outgoing request. Step-by-step Procedure for making MLA Request:

- Forwarding the information to the Central Authority of India. The Investigating Agency or State Government/UT forwards a self- contained proposal with the recommendation of DOP/Law Officer and approval by Director/State Government to IS-II Division, MHA.
- Issue of Request by Central Authority. The IS-II Division, MHA examines and compares the draft along with the relevant documents and prepares an MLA Request. The MLA request is signed by the officer designated at IS-II Division, MHA and is transmitted along with a forwarding letter to the Central Authority of the Requested Country.
- Whenever the request is directly transmitted to the Central Authority of the Requested Country, the Embassy of India or the High Commission of India (whichever is applicable) and AD (IPCC), CBI is to be provided with a copy of the request for maintaining data/records and to follow-up upon the execution of a request.
- After Central Authority of India forwards the Request to Foreign Country:
    a. After transmission of the request to the foreign country, the IS-II Division, MHA (Central Authority of India) either directly or through AD (IPCC), CBI takes the follow-up action for execution of the Request by making correspondence with the Indian Mission abroad or Central Authority of the foreign country.
    b. The Central Authority of the foreign country/Mission may directly communicate with the Central Authority of India or through AD (IPCC), CBI or the contact person of Investigating Agency in case it seeks clarification, additional material, etc., concerning to the request made.
    c. If the communication is made to IS-II Division, MHA, then on receiving such communication, the IS-II Division, MHA would obtain the required clarifications, additional materials, etc., from the Investigating Officer concerned and transmit the same to the foreign country either directly or through diplomatic channels and a copy of such communication is marked to AD (IPCC), CBI for maintaining record and follow-up.

or

    d. If the request is received by AD (IPCC), CBI, then AD (IPCC), CBI would obtain the required clarifications, additional materials, etc., from the Investigating Officer concerned and transmit the same to the foreign country either directly or through diplomatic channels and a copy of such

communication is marked to IS-II Division, MHA for maintain record and follow-up.

or

e. On receiving such communication by Investigating Agency, the contact person of Investigating Agency would obtain the required clarifications, additional materials, etc., from the Investigating Officer concerned and transmit the same to the foreign country, directly, in urgent cases and in all other circumstances the communication is made through IS-II Division, MHA.

iv) After executing the request, the foreign country may forward the Execution Report to IS-II Division, MHA or AD (IPCC), CBI or Indian Mission/Embassy along with the evidence and supporting material. The same is then forwarded to Investigating Agency or State Government/UT.

v) On receipt of execution report, the Investigating Agency or State Government/UT promptly informs the IS-II Division, MHA (Central Authority) about the execution of request and shortcomings if any.

vi) In the case that new facts have come to light after having received the Execution Report, and it is felt by the Investigating Agency that seeking further information from the concerned country is necessary, a supplementary request may be sent. The procedure for making a supplementary request is the same as that of sending any other request.

**Can a court order or a search warrant be issued for data preservation by foreign service providers? If not, what are the reasons?**

For an incoming request, it is not explicitly required by the law, while for an outgoing request all the evidence shall be authenticated by the competent authority.

According to CrPC-Section 166B, all the evidence taken or collected under sub-section (1), or authenticated copies thereof or the thing so collected, shall be forwarded by the Magistrate or police officer, as the case may be, to the Central Government for transmission to the Court or the authority issuing the letter of request, in such manner as the Central Government may deem fit.

*5.1.2. Requests for voluntary disclosure*

| India |
| --- |
| **What legal framework(s) is/are applicable, if any?** |

| |
|---|
| It is not explicitly defined within Indian legislation whether it is possible make a disclosure request directly to service provider based in a foreign country. |
| **Which authority(ies) in your country is/are allowed to request data disclosure to foreign service providers?** |
| The authorities allowed to request data disclosure are not explicitly defined within Indian legislation. |
| **If the requested foreign service providers are prohibited or limited to voluntarily disclose the data, are there any alternative options to obtain the data, e.g. through police-to-police cooperation, specialized networks (e.g. G7/8 24/7 Network) or MLA?** |
| Requests can be made through Interpol or police-to-police channels and spontaneous information sharing is always granted under Art. 18 (4) and (5) of the United Nations Convention against Transnational Organized Crime. |
| **Can a court order or a search warrant be issued for data disclosure by foreign service providers? If not, what are the reasons?** |
| It is not explicitly defined within Indian legislation. |

5.2. Requests sent by your central authority for **Mutual Legal Assistance (MLA)**

| India |
|---|
| **What is your central authority to send requests for MLA in criminal matters?** |
| MLA can be sent to the contact point or agency or via diplomatic channel. All incoming requests are received by Central Authority of India. Letters rogatory on the collection of evidence must be submitted and delivered through diplomatic channels. |
| **Are informal contacts with the central authority of the requested states allowed and used?** |
| For getting informal information or leads, the assistance can be sought through INTERPOL Channels. The Investigating Agency is required to take up the matter with |

Assistant Director, NCB, Central Bureau of Investigation, 5-B, CGO Complex, Lodhi Road, Jawaharlal Nehru Stadium Marg, New Delhi-110003.

A request for assistance shall be made in writing. However, in urgent circumstances, a request may be made orally or by email or facsimile or any other agreed forms of electronic media or through INTERPOL but shall be confirmed in writing by the Investigating Agency or State Government/UT concerned with all relevant documents within 5 days after making such request to IS-II Division, MHA.