INTERPOL

THE USE OF DIGITAL EVIDENCE IN PROSECUTIONS IN ASIA

A comparative study of the laws and policies governing the admissibility and use of digital evidence in criminal proceedings in

Bangladesh
Bhutan
Brunei
Cambodia
Maldives
Mongolia
Nepal
Sri Lanka
Vietnam

EXECUTIVE SUMMARY

NORWEGIAN MINISTRY OF FOREIGN AFFAIRS

HKU LAW

February 2022

Acknowledgements

This project is part of INTERPOL's Project LEADER, which is generously supported by the Norwegian Ministry of Foreign Affairs. The HKU research team would like to thank the members of the INTERPOL Project LEADER team and the members of the INTERPOL Digital Forensics Laboratory for all their assistance with and contributions to this research report. The HKU and INTERPOL teams would like to thank the members of the INTERPOL National Central Bureaus of Bangladesh, Bhutan, Brunei, Cambodia, Maldives, Mongolia, Nepal, and Sri Lanka, who provided written responses to the NCB questionnaire. We would also like to thank the prosecutors in Bangladesh, Bhutan, Brunei, Maldives, Nepal, and Sri Lanka for their responses to the questionnaire for prosecutors. Finally, we would like to thank Mr. Basil Manoussos, Manager of the Cyber Academy, for taking the time to meet with us and share his experience of digital evidence in investigations.

About this Report

The research carried out for this report was primarily based on information gathered from desktop computer searches, sometimes by accessing the databases available in the HKU Libraries' online system. As the members of the research team are not fluent in the non-English official languages of the beneficiary countries, the team was wholly reliant upon materials written in English and English translations of laws and judicial decisions, where available. With the assistance of INTERPOL, separate questionnaires were sent to the INTERPOL National Central Bureau contacts for each of the nine countries and to prosecutors' offices in those countries. Useful information was provided in English in the replies to those questionnaires which covered almost all of the nine countries. Furthermore, some academic experts, whose names are mentioned in the report, were consulted for specific information about some of the jurisdictions. Due to the limits of these research methods, there are likely to be gaps and errors in the information presented in the report. The team welcomes any comments or feedback on the report.

Executive Summary

Digital evidence has become an essential element of criminal investigations and prosecutions for all types of crimes. This research report by The University of Hong Kong, commissioned by the International Criminal Police Organisation, is a study of the laws governing the use of digital evidence in criminal cases in nine beneficiary countries in Asia, namely the People's Republic of Bangladesh, the Kingdom of Bhutan, Brunei Darussalam, the Kingdom of Cambodia, the Republic of Maldives, Mongolia, the Federal Democratic Republic of Nepal, the Democratic Socialist Republic of Sri Lanka, and the Socialist Republic of Vietnam. The report also studies the existing legal arrangements that enable these countries to request and obtain digital evidence from abroad in cross-border cases.

All nine countries are members of the Asia/Pacific Group on Money Laundering, five are members of the South Asian Association for Regional Cooperation (SAARC), four are members of The Commonwealth, and three are members of the Association of Southeast Asian Nations (ASEAN). Six of the countries have mixed common law legal systems, while the other three have civil law systems. The evidence laws of four of the mixed common law jurisdictions are based on or influenced by the Indian Evidence Act of 1872.

This study has found that the laws and practices in all nine countries generally favour the admissibility and use of digital evidence in criminal cases. No instance was found of a court rejecting digital evidence merely on the grounds that the evidence was in a digital form.

In Bangladesh, case law recognises video and audio recorded evidence as falling within the definition of "document" under the Evidence Act (1872). The Speedy Trial Tribunal Act expressly admits electronically recorded evidence, but the court cannot convict the accused on this evidence alone. The Information and Communication Technology Act (2006) (ICTAB) and the Digital Security Act (2018) (DSAB) were enacted to address cybercrime in Bangladesh. The ICTAB clarifies that a statement recorded digitally in electronic form qualifies as a written statement under the Evidence Act. The DSAB put in place procedures to regulate the forensic investigation of digital evidence. The Cyber Tribunal, created by the ICTAB, can admit "forensic evidence" obtained or collected under the DSAB.

The definition of "evidence" in Bhutan's Evidence Act (2005) includes electronic documents and records. The court may decline to admit an electronic document if a genuine question is raised as to the security or integrity of the electronic document system used to record or store the document. Though hearsay evidence is inadmissible, the court has wide discretionary powers to admit hearsay. The Information, Communications and Media Act (2018) confers legal recognition on data messages and electronic documents.

In Brunei's Evidence Act (2014 edition) the definition of "document" includes any matter recorded, stored, processed, retrieved, or produced by a computer. Though hearsay evidence is inadmissible, both the Evidence Act and the Computer Misuse Act (2007 edition) allow for the admission of statements produced by a computer to prove the truth of the contents, under certain conditions. In assessing the weight to be given to a document produced by a computer, the court should consider all of the circumstances, including whether the information was supplied to the computer contemporaneously with the occurrence of the facts the information describes, and whether the person who supplied the information had any incentive to conceal or misrepresent the facts.

Cambodia's Code of Criminal Procedure states that all evidence is admissible unless provided otherwise in law. The Law on Electronic Commerce (2019) provides that digital evidence shall not be rejected in legal proceedings on the sole grounds that the evidence is in the form of an electronic record. A draft Cybercrime Law has yet to be enacted. One decision of the Extraordinary Chambers in the Courts of Cambodia excluded film footage of an alleged interrogation centre because the evidence was repetitive and would have required lengthy investigations into its authenticity.

Although the Maldives Evidence Act (1976) has yet to be updated, the courts will still allow digital evidence when relevant under the terms of this act. A new evidence bill, which provides for the admission of digital evidence, is currently before Parliament.

Mongolia's Criminal Procedure Law (2002) provides that facts and information regarding the circumstances of a crime shall be deemed to be evidence if obtained in accordance with this law. The law recognises audio and video recordings (including photos obtained or produced from these recordings) as "documents", and electronic recordings can be used to corroborate the evidence.

Nepal's Evidence Act (1974) and National Criminal Procedure (Code) Act (2017) were amended in September 2020 to extend the application of certain provisions to audio-visual recordings and digital evidence. The Electronic Transaction Act (2008) confers legal validity on information, documents, records, and other matters stored in digital form. The Information Technology Act (2019) creates new cybercrime offences and enforcement powers.

Sri Lanka's Evidence (Special Provisions) Act (1995) provides for the admissibility of digital evidence such as audio-visual recordings and statements produced by computers. The Electronic Transactions Act (2006) further provides for the admissibility of information contained in a data message, electronic document, electronic record, or other communication. Both laws have provisions allowing the court to presume the accuracy or truth of information contained in an electronic document or record unless the contrary is proved. The Computer Crime Act (2007) created new cybercrime offences and powers to obtain computer data.

Vietnam's Criminal Procedure Code (2015) recognises "electronic data" as a source of evidence. The same law has specific rules for acquiring, storing, preserving, copying, restoring, and displaying electronic data. The findings of expert examinations may be used to explain and present digital evidence. The Law on E-Transactions (2005) provides for the legal validity of data messages.

This study has found that Bangladesh, Bhutan, Brunei, Sri Lanka, and Vietnam have enacted specific laws to facilitate the use of digital evidence in criminal cases, and these laws are a valuable reference for jurisdictions contemplating similar reforms. Cambodia and the Maldives have draft laws which are still going through the legislative process. All countries, except the Maldives, have legal provisions to facilitate the admission of expert opinions as evidence. Such evidence can assist the court in understanding the probative value of digital evidence.

When material digital evidence is located outside the jurisdiction, additional efforts are needed to request and obtain such evidence. Most of the beneficiary countries reported making requests to overseas technology companies such as Facebook to provide account subscriber information. Without any legal compulsion for the companies to co-operate, such requests do not often yield immediate or helpful results.

To provide a legal framework for cooperation, countries enter into binding mutual legal assistance (MLA) arrangements at a bilateral, multilateral, and regional level. The beneficiary countries range from having no bilateral MLA partners (Bhutan and Brunei) to having more than 20 (Vietnam). Bangladesh, Cambodia, Maldives, and Nepal each have fewer than five. Eight of the countries are a party to all three major United Nations (UN) crime suppression treaties, which address respectively drug trafficking, organized crime, and corruption. Bhutan is a party to the treaties on drug trafficking and corruption but not the treaty on organized crime. Parties to these treaties agree to provide one another with MLA as allowed by the domestic law of the requested party. Regarding regional MLA agreements, the members of SAARC, ASEAN, and the Commonwealth have all agreed to MLA arrangements similar to those in the UN treaties, most of which reflect the model UN treaty on MLA.

MLA arrangements are notoriously slow in operational terms and involve multiple layers of authority. Requests are made by and to government central authorities, who must use their domestic laws to process the request. MLA arrangements, to which most of the nine countries are party, provide for assistance with evidence gathering in broad terms and do not oblige parties to have specific measures to preserve and collect computer data efficiently. One exception is the Commonwealth's Harare Scheme, which was revised in 2011 to improve cooperation in digital evidence collection.

Countries who are parties to the Budapest Convention on Cybercrime (e.g., Sri Lanka) or who are members of the Commonwealth's Harare Scheme (e.g., Bangladesh, Brunei, Maldives and Sri Lanka) may be able to assist with specific measures targeting digital evidence. Under the Budapest Convention, parties must afford one another mutual assistance to the widest extent possible for the collection of digital evidence regarding a criminal offence. Parties can request provisional measures such as the expedited preservation of stored computer data and the expedited disclosure of preserved traffic data. A party may request another to search, access, seize, or secure and disclose data stored by means of a computer system. Parties should also have laws in place to enable the real-time collection of traffic data and the interception of content data.

The adoption of the Second Additional Protocol to the Budapest Convention in November 2021 and the enactment of the United States CLOUD Act (2018) shows a clear trend towards creating legal arrangements for states to make direct cross-border requests of private companies and persons for digital data in their control. Non-compliance with such requests may have legal consequences for the company or person concerned. The beneficiary countries should closely follow these developments as they review their own existing MLA arrangements to determine whether they can be made more effective in terms of the timely preservation and collection of cross-border digital evidence. The Second Additional Protocol to the Budapest Convention is expected to be open for signature in May 2022.

This report concludes with references to international guidelines on best practices and standard operational procedures for gathering digital evidence, drafting laws on cybercrime and computer evidence, and reforming MLA arrangements and internal laws to improve co-operation with data requests.

INTERPOL

ABOUT INTERPOL

INTERPOL is the world's largest international police organization. Our role is to assist law enforcement agencies in our 195 member countries to combat all forms of transnational crime. We work to help police across the world meet the growing challenges of crime in the 21st century by providing a high-tech infrastructure of technical and operational support. Our services include targeted training, expert investigative support, specialized databases .and secure police communications channels

:OUR VISION

"CONNECTING POLICE FOR A SAFER WORLD"

Our vision is that of a world where each and every law enforcement professional will be able through INTERPOL to securely communicate, share and access vital police information whenever and wherever needed, ensuring the safety of the world's citizens. We constantly provide and promote innovative and cutting-edge solutions to global .challenges in policing and security