Digital Evidence – The Way Forward: Changes Introduced Under The Bharatiya Sakshya Adhiniyam, 2023

By Priyank Ladoia (Partner)
Tanmay Sharma (Senior Associate)
and Nivedita Mukhija (Senior Associate)

INTRODUCTION

Under Indian law, the evidentiary framework governing criminal as well as civil proceedings was found under the Indian Evidence Act, 1872 ("**IEA**"), which legislation has now been replaced by the Bharatiya Sakshya Adhiniyam, 2023 ("**BSA**") with effect from July 1, 2024. This article aims to highlight and examine key changes introduced vide the BSA in relation to electronic and digital evidence.

ELECTRONIC AND DIGITAL EVIDENCE UNDER THE IEA

The IEA classifies documentary evidence into two categories: (i) primary evidence, being the original document; and (ii) secondary evidence, which may be used to prove the contents of the original document.

In order to bring the colonial-era IEA in line with developments in technology and law, the Indian Evidence (Amendment) Act, 2000 introduced certain changes, such as expanding the definition of documentary evidence to include electronic records.

The Hon'ble Supreme Court has highlighted that the distinction between primary and secondary evidence is also applicable to electronic record (*Arjun Panditrao Khotkar* v. *Kailash Kishanrao Gorantyal*, (2020) 7 SCC 1). Original information contained in the 'computer' is considered as primary evidence, whereas the computer output containing such information is considered to be secondary evidence.

In case the original electronic record is produced in court, the owner of the device in which it is stored may testify before the court and prove that the concerned device, on which the original information is first stored, is owned and/or operated by him. However, in case the electronic record is a part of a 'computer system' or a 'computer network' and it is physically impossible to bring such network or system to the Court, then the only means of proving the information contained in such electronic record is through the mechanism prescribed under Sections 65A and 65B of the IEA. This requirement is also mandatory for providing information to an investigating authority.

While adducing electronic evidence, under Section 65B(4), a certificate authenticating such evidence is required to be submitted by "*a person occupying a responsible official position in relation to the operation of the relevant device or the management of the relevant activities (whichever is appropriate)*". Submission of such a certificate has been held to be a mandatory condition precedent for admitting secondary electronic evidence.

CHANGES INTRODUCED UNDER THE BSA

Electronic Evidence as Primary Evidence

The BSA expressly defines a 'document' to include digital and electronic records, such as, *inter alia*, electronic records on emails, server logs, documents on computers, laptops or smartphones, websites, locational evidence, and voice mail messages stored on digital devices. Therefore, electronic evidence is now classified as primary evidence. The BSA also provides that each stored copy of electronic or digital records, produced from proper custody, is to be considered as primary evidence.

Sections 62 and 63 of the BSA, corresponding to Sections 65A & B of the IEA, retain the criteria of admissibility of electronic evidence, with certain modifications. Under the BSA, the certificate is to be provided by any person in charge of the communication device or management of the relevant activities (whichever is appropriate), as well as an expert. Furthermore, the BSA also provides that such certificate is to be produced at every instance when such evidence is submitted for admission. Such additional requirements may make the process of adducing electronic evidence more onerous, and their purpose remains unclear.

The BSA retains the position espoused in *Arjun Panditrao Khotkar*, wherein primary electronic evidence is admissible *per se*, while secondary electronic evidence is only admissible when accompanied by a certificate attesting the same. However, in light of the fact that copies of electronic evidence, including any temporary files, stored in different devices, may now be considered as primary evidence, it is unclear as to when an electronic evidence would be required to be supported by a certificate under Section 63 of the BSA.

While the certification of electronic evidence by an expert may be a well-intended step towards ensuring that the integrity of the electronic evidence is maintained, it may have been better

reserved for instances wherein there are doubts regarding the authenticity or integrity of the electronic evidence. Further, it is also not clear who would qualify to be such an expert.

Maintenance of Data Integrity

Data integrity has been recognised specifically under the BSA which states that where an electronic or digital record is produced from 'proper custody, such electronic and digital record is primary evidence unless it is disputed. The Schedule to the BSA contains the standard format of the certificate to be produced under Section 63 of the BSA. The certificate by the party tendering the electronic evidence (in Part A) as well as an expert (in Part B) now mandates recording of the hash value of the electronic evidence at the time of submission of such certificate.

One lacuna under the BSA is that it fails to provide adequate safeguards in collection, storing and disposing of electronic and digital evidences during investigation. In a recent case (*Amazon Seller Services Pvt. Ltd. & Anr*. v. *Directorate of Enforcement & Ors*, W.P. (C.) No. 1081 of 2022 (along with batch matters)), the Hon'ble Supreme Court has noted concerns in relation to absence of guidelines for search and seizure of electronic evidence. While such guidelines are awaited, in the interim, the Government has submitted that all investigative agencies will adhere to the CBI Manual. The BSA fails to address this issues, and additionally also does not provide safeguards in relation to dealing with confidential and privileged information that may be collected during investigation.

Other Key Changes

A welcome change introduced under the BSA is that oral evidence now includes any statements given electronically by witnesses as well. This will allow witnesses including experts to record statements, be cross examined and take part in a trial through audio video or other options, therefore allowing more flexibility, convenience and expediting trials in India.

Another notable change is that while the scope of the IEA is limited to India, the BSA removes this limitation, presumably with a view to remove barriers to admissibility of electronic evidence that may be generated or stored outside India.

CONCLUDING REMARKS

The changes introduced under the BSA in relation to electronic evidence indicate a cognizance of the ever-increasing importance of digital evidence in legal proceedings, and are laudable on

that account. However, in practice, they may create more problems than they seek to address. There is an urgent need for clarity on what electronic evidence would constitute primary versus secondary evidence, as only the latter is subject to the requirement of producing an authenticating certificate under Section 63 of the BSA.

The BSA is a missed opportunity as it fails to address several other areas relevant to electronic evidence, such as, *inter alia*, clarifying the proper chain of custody for electronic evidence, providing guidance in relation to the safe storage and disposal of electronic evidence, segregation of privileged and confidential information, and addressing issues in relation to the possibility of self-incrimination which is inherently linked with the seizure of electronic data from a person. While the BSA is a step forward towards establishing a framework for electronic evidence, it is a precarious step, and would benefit from judicial/legislative intervention in order to provide some much-needed certainty.

***