प्रयास
IAS ACADEMY
An Institute For UPSC & BPSC
8818810183 | 8818810184
www.prayasiasacademy.com
prayasiasacademy101@gmail.com
prayasiasacademy

EDITORIAL

E-evidence, New Criminal Law & Its Implementation

Key Points of the Article/Editorial

Background

- The three newly-enacted criminal laws, the Bharatiya Nyay Sanhita (to replace the Indian Penal Code), the Bharatiya Nagarik Suraksha Sanhita (to replace the Code of Criminal Procedure) and the Bharatiya Sakshya Adhiniyam (to replace the Indian Evidence Act) are to come into force on July 1, 2024.
- The Ministry of Home Affairs (MHA) and State governments are preparing for a smooth transition. While some changes have been made in the Bharatiya Nagarik Suraksha Sanhita (BNSS) in connection with investigation and police functioning, a few new offences and some changes introduced in the BNS, the contents of the Indian Evidence Act, 1872 have changed little as far as the Bharatiya Sakshya Adhiniyam (BSA) is concerned.

Clarity on Electronic Record

- There is some precision in the definitions section. An illustration to the definition of "document" (which includes electronic and digital records) says that an electronic record on emails, server logs, documents on computers, laptop or smartphone, messages, websites, locational evidence (should have used the term information in place of evidence), and voice mail messages stored on digital devices are documents.
- Similarly, there is clarity in the provision dealing with primary (electronic) evidence (Section 57) in the form of Explanations. One of such four explanations says that where a video recording is simultaneously stored in electronic form and transmitted or broadcast or transferred to another, each of the stored recordings shall be primary evidence.
- Section 63, which deals with admissibility of electronic records, includes terms such as 'semiconductor memory' and 'any communication device' for better visibility. However, this does not change the impact of the provision because the definition of 'electronic form' given in the Information Technology (IT) Act, 2000 includes information generated, sent, received or stored in 'computer memory'.

Admissibility of electronic Records

- The law on the admissibility of electronic records is settled. Though there are some changes in Section 63 of the BSA (which is equivalent to 65-B of the Indian Evidence Act), the ratio of the Supreme Court judgment in Arjun Panditrao Khotkar vs Kailash Kushanrao Gorantyal & Ors. (2020) will still equally apply to the new provisions.
- In this case, the Court held that the required certificate under Section 65-B(4) - now Section 63(4) of the BSA - is sine qua non for the admissibility of electronic record.

8818810183 | 8818810184
www.prayasiasacademy.com
prayasiasacademy101@gmail.com
prayasiasacademy

- The Court also held that when it is impossible to obey the law, the alleged disobedience of the law is excused. In other words, if it is impossible to produce the required certificate, the court can exempt the mandatory production of the certificate.
- Section 63(4) of the Bharatiya Sakshya Adhiniyam requires the certificate to be signed by two persons instead of one as required under the Indian Evidence Act - the first by the person in charge of the computer or communication device or the management of the relevant activities, and the second, by an expert.
- A standard format of the certificate is also prescribed in the Schedule to the BSA. The expert has to verify the certificate by stating that a particular hash value is obtained by applying a particular hash algorithm. A hash function means an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known as "hash result" such that an electronic record yields the same result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible to reconstruct the original electronic record from the hash result produced by the algorithm.

Preparedness to adopt new format

- While expert certification may help the court in admission of electronic records, it is going to increase the workload of cyber laboratories. There is hardly any crime that does not use a smartphone nowadays. Many crimes are also solved with the help of call records and location information.
- However, if every certificate is to be signed by an expert, the workload will suddenly increase as many cyberlabs may not be equipped with sufficient manpower. Some cyberlabs (such as in Chhattisgarh) are not even notified under the IT Act to give expert opinion on electronic records.
- It would have been reasonable had expert opinion been called for only when the integrity of the seized electronic record is disputed by the opposing party during trial. The courts may, in such cases, always ask for expert opinion.
- It could have been sufficient had the investigating officer ensured that one of the hash algorithms was applied and the message digest was attached with the certificate before it was collected.
- There needs to be a general awareness drive now about the modes and methods of encryption, particularly for private agencies which install closed-circuit televisions on their premises or use other electronic devices for security purposes. Simultaneously, the time before July, must be used by the enforcement agencies to ensure that the required infrastructure is in place to take on the added responsibilities.
- Therefore, the implementation of e-evidence in India's criminal law system presents both opportunities and challenges. While it offers efficiency and speed in investigations and trials, it also raises concerns regarding privacy, data protection, and the digital divide. To effectively navigate these issues, policymakers must ensure robust legal frameworks, technological infrastructure, and capacity building for law enforcement agencies. Additionally, public awareness and engagement are crucial to safeguarding individual rights and promoting trust in the justice system amidst the digital age.