July 2024

Stringent measures against cybercrimes in India's new criminal justice system

On July 1, 2024, India's criminal justice system underwent a significant transformation with the introduction of 3 (three) new laws namely the (a) 'Bharatiya Nyaya Sanhita, 2023' ("**BNS**") replacing the Indian Penal Code, 1860; (b) the 'Bharatiya Nagarik Suraksha Sanhita, 2023' ("**BNSS**") replacing the Code of Criminal Procedure, 1973; and (c) the 'Bharatiya Sakshya Adhiniyam, 2023' ("**BSA**") replacing the Indian Evidence Act, 1872 (collectively referred to as the "**New Criminal Laws**" or "**Legislations**"). These Legislations are intended to operate prospectively, meaning any crime committed until midnight of June 30, 2024, will continue to be governed and prosecuted under the Indian Penal Code, 1860 ("**IPC**"), the Code of Criminal Procedure, 1973, and the Indian Evidence Act, 1872 (collectively referred to as the "**Old Criminal Laws**"). Consequently, the Old Criminal Laws will remain relevant for several years until all pending investigations, inquiries, trials, appeals, and related proceedings are concluded.

With the Old Criminal Laws dating as far back as 1860, the Legislations mark a watershed moment in India's criminal justice system. The New Criminal Laws have introduced provisions aimed at adapting to the complexities of the digital age and deterring crimes that have flourished in the age of the internet. These Legislations also acknowledged the growing digital landscape and incorporated measures to better tackle the increasing rates of cybercrimes in India. While cybercrime is still not defined in the BNS, it is considered a catch-all phrase for offences involving technology such as hacking, phishing, and cyber-stalking.

Inclusion of cybercrime as 'Organised Crime'

A key introduction in the New Criminal Laws is the inclusion of 'Organised Crime' as a separate offence which defines organised crime as criminal activities, including cybercrimes and economic offences, committed by any person or a group of persons acting in concert, singly or jointly, either as a member or on behalf of an organised crime syndicate. With this, BNS envisages and aims to deter cybercriminals acting in groups or on behalf of syndicates which was missing under the IPC. While the IPC addressed cybercrimes like data theft or criminal conspiracy, it did not expressly consider the organised nature of these operations. Further, with such cybercrimes being penalised as organised crimes, punishments for such organised cybercrimes are now more rigorous.

Usage of audio-video communications and electronic communication under various procedures

BNSS has incorporated digital technologies and has expressly mandated use of 'audio-video communications' and 'electronic communication' in various procedures before the courts aiming to reduce delays in criminal proceedings. This change is brought in to decrease paperwork, reduce errors, and improve accessibility to case information for all parties involved. Under BNSS, witnesses and accused individuals can receive summonses through electronic

communication, investigating officers are authorised to record statements using audio-video technology, search and seizure operations can be recorded using audio-video equipment and even trials, inquiries, appeals and related proceedings, may be conducted via electronic mode. This implementation of electronic communications can streamline investigations and lead to faster enforcement against all crimes including cybercrimes.

Scope of certain sections extended to include activities performed through electronic platforms as crimes

Certain sections of BNS, such as those dealing with extortion, forgery or hate speech etc., have been expanded to include such crimes being committed electronically via messages or social media platforms. Therefore, texts, emails, and social media posts sent by a person can be the basis on which that person is convicted for such crimes.

As an example, laws against hate speech (under Sections 196 and 197 of BNS) and laws against spreading misinformation that could disrupt public order (under Section 353 of BNS) have been extended to include electronic communication as the medium for triggering such offences. This allows authorities to prosecute individuals who spread hate or incite violence through social media or other online forums and helps in better enforcement against the growing problem of fake news and online propaganda that can lead to social unrest. Further, definitions such as the meaning of obscene material under Section 294 of BNS have been expressly extended to include content shared electronically, such as revenge porn or violent videos.

Through this expansion of expressly mentioning electronic communication in certain key sections, BNS has aimed to strengthen the legal framework and ensure that cybercriminals who exploit technology are identified faster and do not escape punishment. Furthermore, BNS has referenced the Information Technology Act, 2000 and BNSS for definitions of technological terms that are not expressly defined but used in BNS. This broader scope in recognising criminal activity across various electronic platforms will enhance detection and deterrence of cybercrimes.

Recognition of electronic records as primary evidence

Section 57 of the BSA marks a significant reform towards tackling cybercrimes in India. This section recognises electronic records, encompassing digital documents, emails, social media posts, and more, as primary evidence in court proceedings. This represents a major leap forward from the past, where such evidence held a secondary status, requiring additional verification. Previously, relying on physical copies of digital evidence would significantly delay investigation and prosecution proceedings. However, Section 57 eliminates this barrier by granting electronic records primary evidence status. This allows courts to readily consider electronic records, potentially leading to faster and efficient disposal of cases, particularly in cybercrime scenarios where digital photographs, videos, and other multimedia evidence are often the key pieces of evidence and play a vital role in many cybercrime investigations.

While section 57 of BSA recognises electronic records as primary evidence, section 63 of the BSA outlines the safeguards and provides specific guidelines for the admissibility of such evidence wherein electronic records are required to meet specific authenticity criteria before being admitted in court. Under section 63 of BSA, an electronic evidence is required to comply with the following key conditions to be admissible in a court of law: (a) the computer system that generated the record must have functioned properly during the relevant period; (b) information similar to the electronic record in question must be routinely entered into the system; (c) the electronic record must accurately reflect the data entered into the system; and (d) the computer system must have been used for a legitimate business or activity during the relevant period. Further, the section acknowledges that information may be processed on multiple devices working together and treats such interconnected devices as a single unit for the purpose of meeting the admissibility criteria. Lastly, to introduce electronic records as evidence, a certificate needs to be submitted which is required to be signed by the person in charge of the computer or communication device or management of the relevant activities (whichever is appropriate) and an expert. This certificate is required to state how the record was produced, devices involved, and confirm that the admissibility conditions are met.

This is meant to ensure validity of the electronic evidence and prevent fabricated electronic records from influencing legal proceedings. Digital photographs, videos, and other multimedia evidence play a vital role in many cybercrime investigations. These guidelines establish clear standards for how such evidence can be collected, stored, and presented in court thereby ensuring reliability of such digital multimedia evidence in proving cybercrimes. By streamlining evidence collection, protecting witnesses, and ensuring the integrity of electronic records, this section paves the way for a more effective legal system in combating cybercrime and bringing perpetrators to justice.

Data privacy concerns

The emphasis on digital evidence and e-governance in the New Criminal Laws raises concerns about data privacy of individuals involved in the criminal justice system. While the use of technology can enhance efficiency and transparency, storage of such data also poses risk to individual's privacy rights. It is critical that such digital records are protected from cyber-attacks and data thefts. The government must ensure development of a well-equipped cyber security infrastructure and ensuring that such measures are balanced with strong privacy protection to keep public trust and safeguard individual privacy rights. It is important to note that the Digital Personal Data Protection Act, 2023 ("**DPDP Act**"), published to safeguard personal data, exempts the requirements of notice and consent, among others, for the purposes of prevention, detection, investigation or prosecution of any offence or contravention of any law. For example, under the DPDP Act, an individual has the right to withdraw his consent for processing of personal data but in case of data being processed by the State for purposes such as criminal investigation, such right cannot be exercised against the State.

Conclusion

The enactment of India's New Criminal Laws represents a significant stride towards modernising the country's legal framework, addressing contemporary challenges such as cybercrimes and adapting to the complexities of the digital age. By replacing the Old Criminal Laws, these reforms seek to foster transparency, accountability, and accessibility within the criminal judicial system. However, the successful integration of these laws will hinge upon effective implementation, robust enforcement, and continuous adaptation to societal needs.

Infotech Practice

Our team understands the importance of data privacy in today's digitally interconnected world. We have dedicated our practice to ensuring that your and your customers' personal and business data remains secure, compliant, and respects the sovereignty of individuals and jurisdictions globally.

We prioritise creating bespoke solutions tailored to your business needs. We recognise that every business has unique data privacy challenges, and we use our deep understanding of international and domestic regulations to provide you with the most effective and robust legal strategies. JSA provides advice on highly sophisticated data management, data security and privacy issues. Our depth of experience gives our clients the crucial advantage of consistent and comprehensive, yet practical advice. Our Technology Law Practice group has successfully worked with several multinational organisations for the structuring and roll-out of privacy and information-security programs. We have carried out audit and risk assessments, customised global privacy and information management policies, helped create international data transfer strategies, structure and negotiate complex international data transfer agreements.

This Prism has been prepared by:

Sajai Singh
Partner

Parvathy Manoj
Senior Associate

Himanshu Kumar
Associate

Bhoomika Kumar
Associate

Chambers TOP RANKED Asia-Pacific 2024 JSA

18 Practices and
25 Ranked Lawyers

asialaw OUTSTANDING FIRM 2023-24

19 Practices and
19 Ranked Lawyers

The LEGAL 500

14 Practices and
38 Ranked Lawyers

IFLR1000 TOP TIER FIRM 2023

12 Practices and
42 Ranked Partners
IFLR1000 APAC Rankings 2023

Banking & Finance Team of the Year

Fintech Team of the Year

Restructuring & Insolvency Team of the Year

GCR 100 2024

Recognised in World's 100 best competition practices of 2024

INDIA BUSINESS LAW JOURNAL BEST OVERALL LAW FIRMS 2024 LAW ASIA

Among Top 7 Best Overall Law Firms in India and
11 Ranked Practices
---
11 winning Deals in IBLJ Deals of the Year
---
12 A List Lawyers in IBLJ Top 100 Lawyer List

Employer of Choice 2024

Energy and Resources Law Firm of the Year 2024

Litigation Law Firm of the Year 2024

Innovative Technologies Law Firm of the Year 2023

Banking & Financial Services Law Firm of the Year 2022

7 Ranked Practices,
16 Ranked Lawyers

Elite – Band 1 - Corporate/ M&A Practice
---
3 Band 1 Practices
---
4 Band 1 Lawyers,1 Eminent Practitioner

Ranked #1
The Vahura Best Law Firms to Work
Report, 2022

Top 10 Best Law Firms for Women in 2022

7 Practices and
3 Ranked Lawyers

For more details, please contact km@jsalaw.com

www.jsalaw.com

advocates & solicitors

Ahmedabad | Bengaluru | Chennai | Gurugram | Hyderabad | Mumbai | New Delhi