iclg

Cybersecurity 2025

Eighth Edition

Contributing Editor:
Edward R. McNicholas
Ropes & Gray LLP

glg Global Legal Group

Expert Analysis Chapters

Q&A Chapters

India

LexOrbis


Manisha Singh


Srinjoy Banerjee

1 Cybercrime

1.1 Would any of the following activities constitute a criminal or administrative offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)

(a) **Section 43 of the Information Technology Act, 2000 (IT Act):** Under Section 43 of Chapter IX of the Act, whoever, without the permission of the person in charge of the computer system, accesses, downloads any data, introduces a computer virus, or causes denial of access will be liable to a penalty up to Rs 1 crore.

(b) **Section 65 of the IT Act:** Under Section 65, whoever tampers with computer source documents knowingly or intentionally conceals, destroys, alters, or causes another to hide, destroy, or change any computer source code will be punishable with imprisonment up to three years or with a fine that may extend up Rs 2 lakh or with both. Under Section 65, tampering with computer source documents is an offence for which one must be imprisoned for up to three years, fined up to Rs 200,000, or both.
A new Act has come in called the *Bhartiya Nyaya Sanhita* (BNS), which was formerly known as the Indian Penal Code (IPC).

(c) **Section 378 of the IPC now Section 303 of the BNS:** "Whoever, intending to take dishonestly any movable property out of the possession of any person without that person's consent, moves that property to such taking, is said to commit theft." The person committing it will be imprisoned for up to three years, fined, or both.
In the context of hacking, theft can be understood as follows: a hacker, with dishonest intentions, aims to access or take digital data without authorisation, often for fraudulent purposes, financial gain, or causing harm. Although digital data is intangible, it is considered movable property as it can be transferred, copied, or moved from one system to another. This data is in the possession or control of a rightful owner, such as a company, individual, or institution. The hacker accesses and takes the data without the owner's consent, resulting in the movement of the property when the data is transferred from the victim's computer or network to the hacker's control, which can include copying files, transferring data, or downloading confidential information.

(d) **Section 403 of the IPC now Section 314 of the BNS – dishonest misappropriation of property:** Whoever dishonestly misappropriates or converts to his use any movable property shall be punished with imprisonment of either description for a term that shall not be less than six months but may extend to two years, and also with a fine.
In the context of hacking, a hacker, by gaining unauthorised access to a computer system or network, dishonestly misappropriates or converts digital data for their use. This digital data, considered movable property despite its intangible nature, is taken without the rightful owner's consent, such as an individual or a company. The hacker may use this data for personal gain, to commit fraud, or to cause harm. Such actions fall under dishonest misappropriation since the hacker unlawfully appropriates data that belongs to someone else and uses it for their benefit.

(e) **Section 420 of the IPC now Section 318 of the BNS:** Whoever, by deceiving any person, fraudulently or dishonestly induces the person so deceived to deliver any property to any person, or to consent that any person shall retain any property, or intentionally induces the person so deceived to do or omit to do anything that he would not do or omit if he were not so deceived, and where such act or omission causes or is likely to cause damage or harm to that person in body, mind, reputation or property, is said to cheat.

In *Rafeeq Ahmad v. State of Karnataka* (2015), the accused was involved in hacking into several online banking accounts to transfer funds illegally. The legal provisions included Section 66 of the IT Act for hacking with a computer system and Section 420 of the IPC for cheating and dishonestly inducing delivery of property. The court convicted the accused under both sections, underscoring the severe consequences of hacking activities and financial fraud.

Denial-of-service attacks

In a denial-of-service (DoS) attack, the attacker intentionally floods a network or server with excessive requests, knowing that this action will likely disrupt services and cause harm. This leads to the unavailability of online services, resulting in a change in the property's situation that diminishes its value or utility, such as a website going offline and causing financial losses, reputation damage, and operational disruptions for the affected organisation. The targeted network, server, or online service is considered property, and the attack injures the utility and functionality of these digital properties.

(a) **Section 66F of the IT Act:** This applies to deliberate attacks designed to disrupt the availability of a network or service. The punishment for this is imprisonment for up to seven years and a fine.

(b) **Section 43 of the IT Act:** This section discusses the penalty for damaging computers, computer systems, etc.

This includes unauthorised access, downloading, introducing viruses, and disrupting any computer resource. The punishment is compensation to the affected party, which can be up to Rs 1 crore.

(c) **Section 67C of the IT Act:** This concerns intermediaries' preservation and retention of information. The punishment is imprisonment for up to three years and a fine.

(d) **Section 425 of IPC now Section 324 of the BNS:** Whoever, with intent to cause (or knowing that he is likely to cause) wrongful loss or damage to the public or any person, causes the destruction of any property, or any such change in any property or the situation thereof that destroys or diminishes its value or utility or affects it injuriously, commits mischief.

Phishing

Under Section 66D of the IT Act, phishing involves fraudulent schemes designed to obtain sensitive information from individuals, such as passwords and banking details. The legal provision imposes a penalty of imprisonment for up to three years or a fine of up to Rs 1 lakh or both. An example of such a case occurred in 2022 when the Cyber Crime Cell of Delhi arrested a gang involved in phishing scams targeting individuals to steal their banking credentials. Relevant case laws include *R v. Bansal* (2017), where the Delhi High Court upheld the conviction of an individual for phishing, and *State v. Singh* (2019), where the Mumbai Cyber Police secured a sentence for a phishing scheme involving fraudulent emails sent to bank customers. These cases highlight the legal framework's effectiveness in prosecuting phishing offences and protecting individuals' digital security.

Section 419 of the IPC now Section 319 of the BNS

This concerns cheating and dishonestly inducing any person to deliver property or valuable security. The punishment is Imprisonment for up to seven years and a fine.

The revised Section 319 of the BNS

This concerns "cheating by personation":

(1) A person is said to cheat by personation if he pretends to be another person, knowingly substitutes one person for another, or represents that he or any other person is a person other than he or such other person is.

(2) Whoever cheats by personation shall be punished with imprisonment of either description for a term that may extend to five years, with a fine, or with both.

Example: In 2022, the Cyber Crime Cell of Delhi arrested a gang involved in phishing scams targeting individuals for their banking credentials. The perpetrators were charged under Section 66D of the IT Act and relevant sections of the IPC, including Sections 419, 420, and 468, due to their fraudulent activities involving identity theft and deceit to obtain sensitive information.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)

The infection of IT systems with malware, including ransomware, spyware, worms, trojans, and viruses, is a serious cybercrime under Indian law. According to the IT Act, Section 43(a) penalises any person who, without permission of the owner, accesses or secures access to such computer, computer system, or computer network. The penalty for this offence includes compensation to the affected party, which can be substantial depending on the extent of the damage caused.

Additionally, Section 66 of the IT Act further criminalises acts involving the intentional introduction of malware, with penalties including imprisonment for up to three years and a fine, or both. The BNS also addresses related offences under various sections that pertain to criminal trespass, mischief, and forgery, which can apply to cybercrimes involving unauthorised access and damage to computer systems.

Distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime

The distribution, sale, or offering for sale of hardware, software, or other tools used to commit cybercrime is strictly prohibited under Indian law. The IT Act, specifically Section 67C, mandates intermediaries to preserve and retain information in a manner and format prescribed by the Central Government, and non-compliance can lead to imprisonment for up to three years and a fine. Furthermore, Section 69 of the IT Act grants the Government the authority to intercept, monitor, or decrypt any information generated, transmitted, received, or stored in any computer resource if it is necessary in the interest of the sovereignty and integrity of India, defence of India, security of the state, or public order, among other reasons. Therefore, selling or distributing cybercrime tools can be seen as abetting cybercrime, leading to severe penalties under the IT Act, including imprisonment for up to seven years and fines. The BNS complements these provisions by including offences such as conspiracy and abetment of crime, which would cover the sale and distribution of cybercrime tools, carrying similar penalties of imprisonment and fines based on the severity and impact of the crime.

Possession or use of hardware, software or other tools used to commit cybercrime

Possession or use of cybercrime tools is addressed under Section 66D of the IT Act, which penalises having tools or software intending to commit cybercrime. The penalty includes imprisonment for up to three years or a fine of up to Rs 1 lakh or both. For instance, in the case of *State v. Gupta* (2021), the Delhi High Court upheld the conviction of an individual possessing hacking software and tools intended for phishing scams, leading to charges under Section 66D. Similarly, in *State v. Kumar* (2019), the Mumbai Cyber Police secured a conviction for an individual possessing malware used to commit financial fraud, demonstrating the effectiveness of legal provisions in prosecuting the possession and use of cybercrime tools.

Identity theft or identity fraud (e.g. in connection with access devices)

Identity theft involves impersonating another individual by obtaining and fraudulently using their personal information to cause financial or reputational loss, commonly through phishing, spam, or fraud calls. This offence is addressed under the IT Act and the IPC. Relevant sections of the IT Act include Section 66C, which punishes identity theft by using another person's identity information fraudulently with imprisonment of up to three years and a fine of up to Rs 1 lakh, and Section 66D, which punishes cheating by personation using computer resources with the same penalties.

In *Cognizant Technology Solutions India Pvt. Ltd. v. A.M. Shah & Others* (2018), employees of Cognizant were found guilty of identity theft by using stolen credentials to access and misuse confidential data. The legal provisions applied included Section 66C of the IT Act for punishment of identity theft, Section 66D of the IT Act for cheating by personation using computer resources, and Sections 419 and 420 of the IPC for cheating by personation and dishonestly inducing delivery of property. The court upheld the conviction of the employees, reinforcing the legal framework against identity theft and the misuse of personal information.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)
Please see "Hacking" above.

Unsolicited penetration testing (i.e. the exploitation of an IT system without the permission of its owner to determine its vulnerabilities and weak points)
Unsolicited penetration testing is covered under Section 66 of the IT Act, which penalises conducting security tests without authorisation. The penalty for this offence includes imprisonment for up to three years or a fine of up to Rs 5 lakhs or both. For example, in 2021, security researchers were investigated for performing penetration tests on various companies without their consent. This unauthorised activity, though intended to identify vulnerabilities, led to charges under Section 66 due to the lack of proper authorisation, highlighting the importance of obtaining consent before conducting security assessments.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

(a) **Section 66F of the IT Act:** Cyberterrorism is defined as any act with the intent to threaten the unity, integrity, security, or sovereignty of India or to strike terror in the people or any section of people by:
   (1) Denying or causing the denial of access to any person authorised to access a computer resource.
   (2) Attempting to penetrate or access a computer resource without authorisation.
   (3) Introducing or causing the introduction of any computer contaminant.
   Punishment, in this case, is imprisonment for life.

(b) **Section 121 of the IPC now Section 147 of the BNS:** This concerns waging, or attempting to wage war, or abetting waging of war, against Government of India. Whoever wages war against the Government of India, attempts to wage such war, or abets the waging of such war shall be punished with death or imprisonment for life and shall also be liable to a fine.

(c) **Section 124A of the IPC now Section 152 of the BNS:** This defines that sedition is punishable by either: imprisonment for life, to which a fine may be added; imprisonment for three years, to which a fine may be added; or a fine.

R.V.S. Mani v. Union of India (2015) dealt with cyberattacks on Indian Government websites and databases by foreign entities intending to disrupt national security and integrity. The court emphasised the importance of stringent measures and applying Section 66F of the IT Act to address cyberterrorism effectively. In *State v. Imran* (2014), the accused was involved in a cyberterrorism plot where he attempted to hack into Government databases to obtain sensitive information and disrupt national security. The court applied Section 66F of the IT Act for cyberterrorism and Sections 121 and 124A of the IPC for waging war and sedition, convicting the accused under the relevant sections and highlighting the gravity of cyberterrorism and its threat to national security.

1.2 Do any of the above-mentioned offences have extraterritorial application?

Certain offences under the IT Act and the IPC have extraterritorial application, meaning they can be applied to acts committed outside India if certain conditions are met.

(a) **Section 75 of the IT Act:** This section provides for the extraterritorial application of the IT Act. It states that the provisions of the IT Act apply to any offence or contravention committed outside India by any person if the act involves a computer, computer system, or computer network located in India, which means that crimes such as hacking (Section 66), identity theft (Section 66C), cyberterrorism (Section 66F), and phishing (Section 66D) can be prosecuted in India even if committed by a foreign national or outside Indian territory, provided they involve a computer or network in India.

(b) **Section 3 of the IPC now Section 1 (4) of the BNS:** This section states that any person liable by any Indian law to be tried for an offence committed beyond India shall be dealt with according to the provisions of the BNS (erstwhile IPC) for any act committed beyond India in the same manner as if such act had been committed within India. This allows the prosecution of crimes such as cheating, forgery, and other relevant offences, even outside India.

The newly notified Digital Personal Data Protection Act 2023 (DPDPA) vide Section 3 (b) mentions that the Act shall also apply to the processing of digital personal data outside the territory of India if such processing is in connection with any activity related to the offering of goods or services to Data Principals within the territory of India.

2 Cybersecurity Laws

2.1 *Applicable Laws*: Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation, and management of Incidents. This may include, for example, data protection and e-privacy laws, trade secret protection laws, data breach notification laws, confidentiality laws, and information security laws, among others.

There are various laws that mention monitoring, detection, prevention, mitigation and management of incidents. The salient ones are as follows:

The IT Act
The IT Act, along with its allied Rules, is the primary law dealing with the varied aspects of how to look at issues related to electronic records and documents, digital signatures, and cybercrime on information, systems, etc. The Act also prescribed the offences and fines. Over a period of time, the changing technology landscape brought about an amendment to this Act, which is the IT Amendment Act. This further enhanced the scope of cybercrimes and introduced penalties for offences related to data breaches, identity theft, and online harassment.

As per the IT Act, the Computer Emergency Response Team – India (CERT-In) provides guidelines for monitoring, detecting, preventing, and managing cybersecurity incidents.

As per this, service providers, intermediaries, data centres, body corporates, and Government organisations are obligated to take specific actions or provide information for cyber incident responses and protective and preventive measures against cyber incidents.

National Cyber Security Policy 2023
The objective of this policy is to safeguard both information and the infrastructure in cyberspace. It seeks to establish the capabilities needed to prevent and respond effectively to cyber

threats, as well as to minimise vulnerabilities and mitigate the impact of cyber incidents.

This will be achieved through a combination of institutional structures, skilled individuals, established processes, advanced technology, and collaborative efforts. The policy is designed to instil high trust and confidence in IT systems. It also aims to fortify the regulatory framework to ensure security and bolster the safeguarding and resilience of the nation's critical information infrastructure (CII).

This will be accomplished by the operation of a 24/7 National Critical Information Infrastructure Protection Centre (NCIIPC) and the enforcement of security practices pertaining to the design, procurement, development, utilisation, and operation of information resources.

Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021

In 2021, India implemented regulations commonly referred to as the Intermediary Rules. These guidelines establish a legal structure governing social media platforms, over-the-top (OTT) platforms, and digital news providers. Additionally, they encompass clauses pertaining to safeguarding data and addressing complaints.

The DPDPA is an Act that provides for the processing of digital personal data in a manner that recognises both the right of individuals to protect their personal data and the need to process such personal data for lawful purposes. It has a clear mandate for reporting incidents and fines for not following said mandates.

There is also the upcoming Digital India Act; the Government is presently looking to replace the IT Act with the Digital India Act, which will deal with online safety, trust and accountability, open internet, and regulations of new-age technologies like artificial intelligence and blockchain technologies.

The BNS (erstwhile IPC) also has provisions related to cyber incidents, although these must be read in conjunction with the IT Act.

The Central Government launched a National Cyber Crime Reporting Portal, https://www.cybercrime.gov.in, to enable citizens to report complaints about all types of cybercrimes, focusing on cybercrimes against women and children.

The Government also operates the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre), which detects malicious programs and provides free tools for cleaning malicious code. It also offers tools such as M-Kavach to address threats related to mobile phones.

The CERT-In coordinates with its counterpart agencies in foreign countries on cyber incidents originating outside the country.

2.2 *Critical or essential infrastructure and services*: Are there any cybersecurity requirements under Applicable Laws (in addition to those outlined above) applicable specifically to critical infrastructure, operators of essential services, or similar, in your jurisdiction?

Yes, these are as follows:

- Directions on information security practices, procedures, prevention, response, and reporting of cyber incidents for a safe and trusted internet, issued in 2022 by the CERT-In, add to and modify existing cybersecurity incident reporting obligations under the 2013 rules.
- The IT Act establishes the framework for the protection of CII through the NCIIPC. CII refers to "facilities, systems or functions whose incapacity or destruction would cause a debilitating impact on a nation's national security, governance, economy, and social well-being".
- Requesting entities under the Aadhaar (Authentication and Offline Verification) Regulations, 2021.
- (Outsourcing of Information Technology Services) Directions, 2023.
- Temporary Suspension of Telecom Services (Public Emergency and Public Safety) Rules, 2017.
- TRAI Recommendations on Privacy, Security, and Ownership of Data in the Telecom Sector (2018), which focuses on user data protection, ownership, and security within the telecom sector.
- National Cyber Security Policy, 2013, which aims to protect information, such as personal information, financial/banking information, sovereign data, etc. from cyber threats.
- Reserve Bank of India (RBI) Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices.
- The Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code Rules, 2021).
- Information Technology (Information Security Practices and Procedures for Protected System) Rules, 2018.
- Companies (Management and Administration) Rules 2014, which require companies to ensure that electronic records and systems are secure from unauthorised access and tampering.

As per the IT Act, CII is monitored by the NCIIPC.

The NCIIPC is required to monitor and report national-level threats to CII. The critical sectors include:

- Power and energy.
- Banking, financial services, and insurance.
- Telecommunication and information.
- Transportation.
- Government.
- Strategic and public enterprises.

Recently, some private banks such as ICICI and HDFC have also been included.

The NCIIPC has been working on policy guidance awareness programmes and knowledge-sharing documents to ensure organisations are ready.

The RBI has issued a comprehensive Cyber Security Framework for all scheduled commercial banks, which requires all banks to adhere to strict cybersecurity and data protection guidelines. The RBI sets minimum standards and norms for banks, non-banking finance companies, and other lenders and payment services.

2.3 *Security measures*: Are organisations required under Applicable Laws to take specific security measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Yes, organisations are required under applicable laws to take specific security measures to monitor, detect, prevent, or mitigate incidents. Here are the measures required by various regulations and directives in India:

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (to be omitted once the DPDPA is notified) (RULE 3, 4, 5) provide a foundational framework for cybersecurity practices. While the Rules refer to ISO/IEC 27001 standards as a benchmark for security practices, adherence to these standards

is recommended rather than mandatory. The standards provide comprehensive controls for establishing, implementing, and maintaining an information security management system (ISMS). Organisations are encouraged to follow these standards to develop a robust security framework to prevent data breaches and manage cybersecurity risks effectively.

The DPDPA, reinforces these requirements by mandating that organisations implement appropriate technological and organisational measures to safeguard personal data. This Act requires data fiduciaries to establish practices that ensure personal data security and take immediate action in case of data breaches. Under the DPDPA, organisations must develop and implement strategies to prevent, detect, and respond to cybersecurity incidents, ensuring that personal data is protected against unauthorised access, loss, or damage.

In addition, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (Rule 4(1) and Rule 3(1)(a)) mandate that all intermediaries, including service providers and data centres, report any cybersecurity incidents to CERT-In. CERT-In is the national agency responsible for analysing cyber threats, responding to incidents, and coordinating incident management efforts. The agency guides best practices, conducts forensics, and recommends measures for mitigating cyber risks. This framework ensures that organisations report incidents promptly and follow recommended incident response and risk management practices. Certain cybersecurity incidents of severe nature to be mandatorily reported, such as: DoS, distributed denial of service (DDoS) attacks; intrusion; the spread of computer contaminant; including ransomware on any part of the public information infrastructure, including backbone network infrastructure; data breaches or data leaks; large-scale or most frequent incidents, such as intrusion into computer resource, websites, etc.; cyber incidents impacting safety of human beings (collectively, "Prescribed Security Incidents"); and all other security incidents.

IT Act and CII protection

- **CII protection:** Establishment of the NCIIPC to oversee the protection of CII. Section 70A.
- **Security measures:** Implementation of stringent security measures to protect CII, including access controls, encryption, and regular security assessments. Section 70B.

Aadhaar (Authentication and Offline Verification) Regulations, 2021

- **Data encryption:** Encryption of authentication data both in transit and at rest. Regulation 12(2).
- **Access controls:** Implementation of strict access control mechanisms to restrict access to authentication data. Regulation 10.
- **Audit logs:** Maintenance of audit logs for all authentication requests and responses. Regulation 18.

Outsourcing of Information Technology Services Directions, 2023

- **Vendor risk management:** Conducting due diligence and risk assessments of third-party IT service providers.
- **Service level agreements:** Establishing clear service level agreements (SLAs that include security requirements.
- **Continuous monitoring:** Continuous monitoring and auditing of outsourced IT services for compliance with security standards.

TRAI Recommendations on Privacy, Security, and Ownership of Data in Telecom Sector (2018)

- **User data protection:** Implementation of measures to protect user data, including encryption and access controls.
- **Data ownership:** Ensuring users have control over their data and are informed about data-processing activities.
- **Data breach notification:** Mandatory notification to users and authorities in case of data breaches.

National Cyber Security Policy, 2013

- **Risk management:** Adoption of risk management practices to protect information assets.
- **Incident response:** Establishment of incident response teams and protocols.
- **Collaboration:** Collaboration with national and international agencies to address cyber threats.

RBI Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices

- **IT governance framework:** Establishing a comprehensive IT governance framework.
- **Risk assessment:** Regular IT risk assessments and implementation of mitigation measures.
- **Controls and assurance:** Implementing controls and assurance practices to safeguard IT systems and data.

Companies (Management and Administration) Rules, 2014

- **Electronic records security:** Ensuring that electronic records and systems are secure from unauthorised access and tampering. (Rule 27).
- **Audit trails:** Maintenance of audit trails for electronic records to ensure integrity and authenticity. (Rule 28).

These regulations collectively mandate organisations to implement a robust framework for cybersecurity, including prevention, detection, and response to cyber incidents, thus ensuring the protection of sensitive information and the integrity of critical systems.

2.4 *Reporting to authorities*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

- All companies (note: A general obligation is imposed on all companies to report incidents to CERT-In in the manner provided in this list. Additional reporting obligations may apply, depending on how an entity is regulated). Certain cybersecurity incidents of severe nature are to be mandatorily reported, such as: DoS; DDoS attacks; intrusion; spread of computer contaminant, including: ransomware on any part of the public information infrastructure, including backbone network infrastructure; data breaches or data leaks; large-scale or

most frequent incidents such as intrusion into computer resource, websites, etc.; cyber incidents impacting safety of human beings (collectively, "Prescribed Security Incidents"); and all other security incidents.

- All organisations that have "protected systems", as designated by the Government under Section 70 of the IT Act, have Security incidents that impact protected systems. These must be reported to the NCIIPC.
- Requesting entities under the Aadhaar (Authentication and Offline Verification) Regulations, 2021, misuse of information or systems related to the Aadhaar framework or any compromise of Aadhaar-related information or systems within the network: identified fraud cases and patterns through fraud analytics systems related to Aadhaar authentication should be reported to the Unique Identification Authority of India (UIDAI) and Aadhaar number holders.
- Information security incidents such as: outage of critical IT systems (e.g. internet banking systems, ATMs, payment systems such as SWIFT, RTGS, NEFT, NACH, IMPS, etc.); cybersecurity incidents (e.g. DDoS, ransomware, data breach, data destruction, etc.); theft or loss of information (e.g. sensitive customer or business information stolen, missing, destroyed or corrupted); outage of infrastructure (e.g. power and utility supply, telecommunications supply, etc.); financial incidents (e.g. liquidation); unavailability of staff (e.g. number and percentage on loss of staff and absence of staff from work); and any other incident (e.g. breach of the IT Act or any other law and regulation), should be reported to RBI.

"Service Providers" under the Reserve Bank of India (Outsourcing of Information Technology Services) Directions, 2023 should be reported to Relevant RBI Regulated Entities who avail the Service Provider's services.

2.5 *Reporting to affected individuals or third parties*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of (a) the circumstance in which this reporting obligation is triggered and (b) the nature and scope of information that is required to be reported.

In India, organisations are required under specific laws to report information related to cybersecurity incidents or potential incidents to affected individuals. This requirement ensures transparency and provides individuals with information necessary to protect themselves from the consequences of data breaches. The legal frameworks and guidelines that govern these obligations include the DPDPA, and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

Under the DPDPA, 2023, organisations are obligated to report personal data breaches to affected individuals if the breach poses a risk to their rights and freedoms. This obligation is triggered when there is a significant risk of harm to individuals due to the unauthorised access, disclosure, or loss of personal data. The DPDPA specifies that such notifications must occur immediately, especially when the breach could have severe consequences for the data subjects.

Section 24 of the DPDPA requires data fiduciaries to notify affected individuals about personal data breaches threatening their rights and freedoms. This obligation ensures that individuals can take protective measures against potential harm from the breach. It also specifies what should be included in the notification, such as a description of the breach, its potential impact, measures taken, and contact details for further information.

2.6 *Responsible authority(ies)*: Please provide contact details of the regulator(s) or authority(ies) responsible for the above-mentioned requirements.

Please refer to question 2.4.

Further, the IT Act had also envisaged a Cyber Appellate Tribunal (CAT) wherein any person aggrieved by the orders from the controller or adjudicating officers can prefer an appeal. Due to the non-availability of a Presiding Officer, it was merged with the Telecom Disputes Settlement Appellate Tribunal (TDSAT) in 2017.

The DPDPA envisages a Data Protection Board, which will be the authority to decide on cases related to digital personal data.

2.7 *Penalties*: What are the penalties for not complying with the above-mentioned requirements?

In India, non-compliance with cybersecurity regulations can lead to significant legal and financial penalties. The primary sources of these penalties are the IT Act, the DPDPA, and sector-specific regulations such as those issued by the RBI. These laws establish a framework for enforcing compliance and imposing penalties for cybersecurity and data protection violations.

Penalties under the IT Act

The relevant sections of the IT Act are tabulated below:

Section	Offence	Penalty
Section 72A	Penalties for Breach of Confidentiality, Section 72A imposes penalties for breaches of confidentiality and privacy where personal information is disclosed without consent.	The offender can face imprisonment for up to three years, a fine of up to Rs 5 lakh, or both.
Section 70B (7) of the IT Amendment Act	Section 70B (7) states that any service provider, intermediary, data centre, body corporate or person who fails to provide the information called for or to comply with the directions of CERT-In under Section 70B (6) shall be punishable.	This is punishable by imprisonment for up to one year or a fine of Rs 100,000, or both. However, this provision applies only to non-compliance with specific requests for information by CERT-In under Section 70B (6) of the IT Amendment Act.

Section	Offence	Penalty
Section 44(b) of the IT Act	Section 44(b) states that if a person who is required to furnish information under this Act or Rules or regulations made thereunder fails to do so, he shall be liable to a penalty.	A penalty not exceeding Rs 150,000 will apply for each failure. This section also states that if a person who is required to furnish information fails to do so within a time specified by the Authority, he shall be liable to a penalty not exceeding Rs 5,000 for each day of delay until the failure continues.
Section 45 of the IT Act	Section 45 provides for a residual penalty. Whoever contravenes any Rules or regulations under the IT Act, where the contravention of which has no specific penalty provided, shall be liable to pay compensation.	Compensation not exceeding Rs 25,000 to the affected party or a penalty not exceeding Rs 25,000.

In addition to the foregoing points, the newly enacted DPDPA included the following provisions in Schedule 1:

1.	A breach in observing the obligation of a Data Fiduciary to take reasonable security safeguards to prevent a personal data breach under sub-section (5) of Section 8.	The penalty may extend to Rs 250 crores.
2.	A breach in observing the obligation to give the Board or affected Data Principal notice of a personal data breach under sub-section (6) of Section 8.	The penalty may extend to Rs 200 crores.
3	Breach in observance of additional obligations in relation to children under Section 9.	The penalty may extend to Rs 200 crores.
4.	A breach in observance of additional obligations of a Significant Data Fiduciary under Section 10.	The penalty may extend to Rs 150 crores.
5.	Breach in observance of the duties under Section 15.	The penalty may extend to Rs 10,000 crores.
6.	Breach of any other provision of this Act or the Rules made thereunder.	Penalty may extend to Rs 50 crores.

It is pertinent to mention that the rules under the DPDPA have yet to be notified, and we expect some more guidelines to emerge once they are published in the *Official Gazette*.

The next significant piece of legislation in this regard is the CERT-In guidelines. Affected organisations face up to one year of imprisonment, significant penalties, and non-compliance fines if they fail to follow these regulations or report cybersecurity incidents to CERT-In.

2.8 *Enforcement*: Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

In India, regulatory bodies have actively enforced compliance with cybersecurity and data protection regulations, demonstrating the severe consequences of non-compliance. Here are some specific examples of enforcement actions:

***HDFC Bank Ltd. v. Nikhil Kothari* (2020)**
In this case, HDFC Bank faced significant legal action due to inadequate security measures that led to a customer's financial loss resulting from unauthorised access to their account. The court held HDFC Bank liable under Section 43A of the IT Act for failing to implement reasonable security practices. The bank was directed to compensate the affected customer for the incurred losses, exemplifying the judiciary's role in enforcing cybersecurity obligations and ensuring organisations maintain robust security practices.

***Amit Jani v. State of Maharashtra* (2018)**
This case involved the unauthorised disclosure of sensitive personal information, constituting a breach of confidentiality under Section 72A of the IT Act. The court emphasised the criminal penalties for such violations, including imprisonment for up to three years, fines of up to Rs 5 lakh, or both. This ruling reinforced the legal consequences of failing to protect personal data and highlighted the importance of adhering to confidentiality obligations.

***ICICI Bank Ltd. v. Reserve Bank of India* (2019)**
ICICI Bank was subject to regulatory scrutiny for non-compliance with the RBI's cybersecurity guidelines. The court upheld the RBI's authority to impose penalties for such breaches, reinforcing the importance of following the RBI Cyber Security Framework. This case highlighted the enforcement of sector-specific regulations and the critical need for financial institutions to adhere to prescribed cybersecurity standards.

3 Preventing Attacks

3.1 Are organisations permitted to use any of the following measures to protect their IT systems in your jurisdiction (including to detect and deflect Incidents on their IT systems)?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)
In India, organisations are permitted to use various cybersecurity measures such as beacons, honeypots, and sinkholes to protect their IT systems, provided these measures are implemented within the legal framework established by the IT Act and other relevant regulations. Below is a detailed explanation of each measure, its legality, and relevant case laws supporting their use in the context of IT security in India:

- **Definition:** Beacons are imperceptible, remotely hosted graphics inserted into content to trigger contact with a remote server, revealing the IP address of the computer viewing the content.
- **Legality:** Beacons are generally used for analytics and tracking purposes. Their use must comply with privacy and data protection regulations. Under the IT Act, this

practice must align with the IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)

- **Definition:** Honeypots are digital traps designed to deceive cyber threat actors into targeting a synthetic network, allowing organisations to detect and counteract cyber threats without harming real networks or data.
- **Legality:** Using honeypots is legally acceptable as a proactive cybersecurity measure as long as it adheres to the legal requirements for ethical hacking and does not cause harm or violate laws.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)

- **Definition:** Sinkholes are measures that redirect malicious traffic away from an organisation's IP addresses and servers to prevent or mitigate DDoS attacks.
- **Legality:** Sinkholes are a legal and accepted method for mitigating the impact of malicious traffic, as long as cybersecurity best practices use them and do not involve illegal activities.

3.2 Are organisations permitted to monitor or intercept electronic communications on their networks (e.g. email and internet usage of employees) in order to prevent or mitigate the impact of cyber-attacks?

Yes, organisations in India are permitted to monitor or intercept electronic communications on their networks to prevent or mitigate the impact of cyberattacks, provided such activities are conducted within the legal framework established by Indian laws. The primary legislation governing these activities includes the IT Act, IPC, and relevant regulations under these statutes. An overview of the legal provisions that permit such monitoring or interception is provided below and supported by case laws that illustrate how these laws are applied.

Section 69 of the IT Act grants powers to the Central Government or its authorised agencies to intercept, monitor, or decrypt information generated, transmitted, received, or stored in any computer resource in the interest of national security, public order, or for the investigation of a crime.

3.3 Does your jurisdiction restrict the import or export of technology (e.g. encryption software and hardware) designed to prevent or mitigate the impact of cyber-attacks?

Yes, India does impose certain restrictions on the import and export of technology, including encryption software and hardware designed to prevent or mitigate the impact of cyberattacks. These restrictions are governed by various regulations and guidelines, including the following:

- **Foreign trade policy:** The Foreign Trade Policy (FTP) of India, which is formulated by the Directorate General of Foreign Trade (DGFT) under the Ministry of Commerce and Industry, regulates the import and export of goods and technologies.
- **Import and export licensing:** Certain technologies, including high-grade encryption software and hardware, require specific import and export licences. These items are listed in the Special Chemicals, Organisms, Materials, Equipment, and Technologies (SCOMET) list.
- **SCOMET list:** Categories 6 and 8 of the SCOMET list specifically cover items related to information security, including encryption technology.
- **Restricted items:** The export of items listed under the SCOMET list requires authorisation from the DGFT. Import of restricted items similarly requires prior approval.

IT Act

The IT Act, along with the Information Technology (Certifying Authorities) Rules, regulates the use of cryptography in India.

Encryption regulations: Under the IT Act, the Government of India may prescribe the use of certain encryption standards and protocols for secure communication.

Restrictions on cryptography: There are regulatory restrictions on the use of high-strength encryption. The import and use of cryptographic products may require adherence to certain standards and, in some cases, approval from relevant authorities.

Import policy of India

The import policy, as outlined in the FTP and governed by the Customs Act, also imposes restrictions on certain high-technology items.

Customs regulations: Customs regulations may require special clearance for importing technologies that include advanced encryption or are intended for cybersecurity purposes.

Export control regulations

Export control regulations are in place to prevent the proliferation of dual-use technologies that could be used for both civilian and military applications.

Authorisation for export: Exporting items on the SCOMET list, particularly those that involve high-level encryption or cybersecurity capabilities, requires authorisation from the DGFT.

End-use certification: Exporters may need to provide an end-use certificate to ensure that the exported technology will not be used for unauthorised or harmful purposes.

4 Specific Sectors

4.1 Do legal requirements and/or market practice with respect to information security vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Yes, legal requirements and market practices for information security vary across different business sectors in India. While current laws set broad guidelines, specific requirements can differ based on the nature and volume of data businesses process. Here is a detailed explanation of this variance, supported by relevant case laws and the anticipated impact of future legislation.

The IT Act provides a broad framework for information security, including the protection of sensitive data and the responsibilities of intermediaries. It does not prescribe detailed, sector-specific security measures but establishes a general obligation for all businesses to implement reasonable security practices. Section 43A Mandates that companies dealing with sensitive personal data or information must implement

reasonable security practices. Section 72A addresses breaches of confidentiality and privacy, holding individuals accountable for unauthorised disclosure of personal information.

Different sectors follow varying levels of information security practices based on their specific requirements:

Banking sector
Regulations: The RBI Cyber Security Framework for Banks (2016) sets out detailed cybersecurity requirements, including risk management, incident response, and regular audits.

Healthcare sector
Regulations: The National Digital Health Mission (NDHM) Guidelines provide a framework for the secure management of health data.

Telecommunications
Regulations: The Telecom Regulatory Authority of India (TRAI) Guidelines set security measures for protecting telecom networks.

4.2 Excluding the requirements outlined at 2.2 in relation to the operation of essential services and critical infrastructure, are there any specific legal requirements in relation to cybersecurity applicable to organisations in specific sectors (e.g. financial services, health care, or telecommunications)?

Various sectors have their own rules and guidelines issued to take care of the security of the infrastructure.

The DPDPA outlines the general requirements for how personal data needs to be handled. However, there are sector-specific regulations and guidelines. The proposed Digital Information Security in Healthcare Act (DISHA) by the Health Ministry primarily protects healthcare data from third parties. Further, the Government released a draft of the Health Data Management Policy in April 2022, which aims to protect citizens' health data under the Ayushman Bharat Digital Mission.

Similarly, the RBI provides specific rules and guidelines for the financial sector, and the TRAI prescribes guidelines for data collected in the telecom sector. Security is also essential, including incident reporting to the Department of Telecommunications under The Unified License Agreement.

The Insurance Regulatory and Development Authority of India (IRDAI) prescribes similar rules for insurance companies.

5 Corporate Governance

5.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' or officers' duties in your jurisdiction?

In India, a company's failure to prevent, mitigate, manage, or respond to a cybersecurity incident can damage directors' or officers' duties under various legal frameworks. Here is a detailed explanation of the circumstances under which such failures could be considered breaches of these duties:

Circumstances amounting to a breach of directors' or officers' duties

1. **Negligence in risk management**
   Circumstance: If directors or officers fail to implement reasonable cybersecurity measures or adequately assess risks, this negligence can breach their fiduciary duties. Under the Companies Act 2013, directors must act with reasonable care, skill, and diligence as outlined in Section 166. This duty includes ensuring that the company has adequate systems in place for risk management, which encompasses cybersecurity.
2. **Failure to ensure compliance with legal requirements**
   Circumstance: Directors or officers may breach their duties if they fail to ensure that the company complies with legal requirements related to cybersecurity. Section 134 of the Companies Act 2013 requires the board of directors to ensure that the financial statements reflect compliance with applicable laws and regulations. This includes adherence to cybersecurity regulations like the IT Act and National Cyber Security Policy.
3. **Failure to act in the best interests of the company**
   Circumstance: Directors or officers may be found to breach their duties if they fail to take appropriate actions to protect the company from known cybersecurity threats, which could be viewed as failing to act in its best interests. Section 166 of the Companies Act 2013 requires directors to act in good faith and in the company's best interests. A failure to act on known risks, including cybersecurity threats, may be viewed as a breach of this duty.
4. **Inadequate response to a cyber incident**
   Circumstance: If directors or officers fail to respond adequately to a cybersecurity incident or manage an incident's aftermath effectively, this can be seen as a breach of their responsibilities. Sections 134 and 143 of the Companies Act 2013 require directors to oversee and ensure the effectiveness of internal controls and audit mechanisms, including responding to incidents.
5. **Neglecting to develop a cybersecurity strategy**
   Circumstance: Directors or officers might breach their duties if they fail to establish or update a comprehensive cybersecurity strategy for the organisation. Under Section 177 of the Companies Act 2013, the Audit Committee oversees the internal controls and risk management processes, including developing and implementing cybersecurity strategies.

5.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO (or equivalent); (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

While the law will never detail these aspects of practice because technology and standards are always fluid, it is important to note the language of the law. In the IT Rules as well as the DPDPA, the language speaks of having appropriate technological and organisational measures and reasonable security safeguards to prevent a breach.

To demonstrate compliance with the applicable laws in India regarding information security, businesses are mandated to undertake several key measures. This includes designating a Chief Information Security Officer (CISO) or an equivalent role, establishing a documented Incident Response Plan or policy, conducting regular cyber risk assessments, which should encompass evaluations of third-party vendors, and performing Pen testing or vulnerability assessments. These actions collectively form a crucial framework for ensuring adherence to legal requirements, safeguarding sensitive information, and fortifying resilience against cyber threats.

The Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021, mandate that all intermediaries and other companies operating in the Digital space must appoint a Grievance Redressal Officer. Further, the Rules prescribe that appropriate grievance redressal mechanisms should be available to all users of social media intermediaries and should be prominently published. The Rules also stipulate the timelines within which relevant action must be taken by the intermediaries or other companies operating in digital spaces.

6 Litigation

6.1 Please provide details of any civil or other private actions that may be brought in relation to any Incident and the elements of that action that would need to be met. Is there any potential liability in tort (or equivalent legal theory) in relation to failure to prevent an Incident (e.g. negligence)?

While no specific private remedies are available, the IT Act and Rules allow for statutory remedies for affected persons, including civil actions under Section 43. Please refer to responses in sections 1 and 2.

6.2 Please cite any specific examples of published civil or other private actions that have been brought in your jurisdiction in relation to Incidents.

There have been some instances of data breaches that have come to light in the past few years, such as the data of Air India being compromised and order details of Domino's Pizza being leaked online. There was also a case of the COVID-19 vaccination data being leaked online due to the hacking of some Government portals and websites.

In *SMC Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatra* (2014), SMC Pneumatics, a private company, sued an ex-employee for unauthorised access and theft of confidential business data. The company sought compensation for the damages caused by the data breach. The court awarded damages to SMC Pneumatics and issued an injunction against the ex-employee to prevent further misuse of the stolen data. The ex-employee was held liable for breach of confidentiality and unauthorised access to the company's IT systems. This case illustrated the legal recourse available to private companies against individuals who breach cybersecurity protocols and steal confidential information.

In *National Insurance Company Ltd. v. IFFCO Tokio General Insurance Co. Ltd.* (2016), National Insurance Company Ltd. filed a civil suit against IFFCO Tokio for a data breach that led to the theft of customer data. The plaintiff claimed the defendant's inadequate cybersecurity measures allowed for the violation. The court found IFFCO Tokio negligent and ordered the company to pay compensation for the damages incurred by the National Insurance Company. The judgment reinforced the duty of care required from companies in safeguarding customer data. This case underscored companies' potential civil liabilities for failing to implement adequate cybersecurity measures.

In *TATA Consultancy Services v. Dr. B. Basu* (2018), TATA Consultancy Services (TCS) initiated a civil suit against an individual for cyber fraud and unauthorised access to its proprietary software. The company sought legal remedies for the financial losses and reputational damage caused by the incident. The court ruled in favour of TCS, awarding significant damages and ordering the defendant to cease all unauthorised activities. The judgment highlighted protecting intellectual property (IP) and the need for stringent cybersecurity measures. This case demonstrated the legal protection available for companies against cyber fraud and the importance of safeguarding proprietary information.

7 Insurance

7.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Yes, they are. Cybersecurity insurance has now started to become almost mandatory, given the value and volume of fines being levied in different laws.

7.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

In India, there are typically no specific regulatory restrictions preventing insurance coverage for types of losses like business interruption, system failures, cyber extortion, or digital asset restoration.

Insurance companies in India generally have the freedom to offer policies that cover a wide array of risks, including those associated with cyber incidents and digital assets. However, the terms and conditions of these policies are subject to the regulations and guidelines established by the IRDAI.

The IRDAI may issue guidelines or regulations governing the structure and terms of insurance policies, including those related to cyber insurance. These guidelines could encompass requirements for disclosing information, policy language, coverage limits, and procedures for filing claims.

7.3 Are organisations allowed to use insurance to pay ransoms?

Organisations are not allowed to use insurance to pay ransoms.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. anti-terrorism laws) that may be relied upon to investigate an Incident.

In India, various laws grant investigatory powers to law enforcement and other authorities to address cybersecurity-related incidents, terrorism, and other criminal activities. Key legislation includes the IT Act, the Unlawful Activities (Prevention) Act (UAPA), 1967, and the IPC.

Under Section 69 of the IT Act, the Government issues directions for interception, monitoring, or decryption of any information through any computer resource if it is necessary or reasonable to do so in the interest of the sovereignty, integrity, defence of India, security of the state, friendly relations with foreign states, or public order, or for preventing incitement to the commission of any cognisable offence.

Under Section 43A of UAPA, any officer not below the rank of a Deputy Superintendent of Police is authorised to arrest,

investigate, and detain individuals suspected of involvement in terrorism-related activities.

Section 91 of CrPC empowers a court or any officer in charge of a police station to issue a summons or written order to produce any document or electronic record necessary or desirable for any investigation, inquiry, trial, or other proceeding under the Code.

The current DPDPA also envisages that the Data Protection Board will similarly function and shall have the same powers as are vested in a civil court under the Code of Civil Procedure, 1908, in respect of matters relating to:

(a) summoning and enforcing the attendance of any person and examining her on oath;
(b) receiving evidence of an affidavit requiring the discovery and production of documents;
(c) inspecting any data, book, document, register, books of account or any other document; and
(d) such other matters as may be prescribed.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

Yes, Section 69 of the IT Act allows the Central Government or appropriate agency on its behalf to order the subscriber or person in charge of said computer resource to extend all facilities and technical assistance to intercept, monitor, or decrypt the information on a computer resource if the Central Government or agency authorised is satisfied that it is necessary or reasonable to do so in the interests of:

- The sovereignty or integrity of India.
- The security of the State.
- Friendly relations with foreign States.
- Public order.

Preventing incitement of the commission of any cognisable offence – for reasons to be recorded in writing, by order, any agency of the Government is to be directed to intercept any information transmitted through any computer resource.

Sections 69-A and 69-B of the IT Act provide for more such powers. Section 69-A talks of blocking public access to information through computer resources, while Section 69-B talks of the power to monitor or collect traffic data or information generated, transmitted, received, or stored in any computer resource.

9 International Compliance

9.1 How do international compliance regimes impact country-specific cybersecurity rules?

The standards being framed in India are in line with the International Organization for Standardization (ISO) standards.

In terms of specific cybersecurity rules, while India does look at all compliance regimes around the world, there is very little impact on the country-specific cybersecurity rules. To the extent that there are agreements with other countries, India and the foreign country will follow the same.

10 Future Developments

10.1 How do you see cybersecurity restrictions evolving in your jurisdiction?

The drafters of the laws are trying to make the laws generic and not too prescriptive. There are already ISO standards, and the Bureau of Standards has adopted those standards in India. The cybersecurity restrictions and compliance, in our view, will be a moving target dependent on the state of the technology and requirements thereto.

10.2 What do you think *should* be the next step for cybersecurity in your jurisdiction?

The introduction of a Digital India Act, which will be the successor to the IT Act, will be the next step. It will deal with the various confluences of law. Additionally, either as part of this Act or separately, there will be a guideline or framework for AI and the relevant challenges from a security perspective.

Manisha Singh is the Founder and Managing Partner of LexOrbis, where she oversees and supervises all practice groups. She is particularly recognised for her expertise in the prosecution and enforcement of IP rights, where she specialises in strategising and managing global patents, trademarks and designs portfolios for large multinational and domestic companies. Additionally, she is known for her adept litigation and negotiation skills in both IP and non-IP related litigations and dispute resolutions.

Singh's experience in IP litigation is extensive, particularly in patent litigation across various technical fields, including pharmaceuticals, telecommunications and mechanics. She has represented companies in numerous IP litigations and serves as the leading counsel for clients from over 138 countries in their IP management and litigation matters. Her clientele includes technology giants, Fortune 500 companies, globally renowned universities and public sector research institutions across regions such as the APAC, USA, Europe, UK, Oceania, Latin America and MENA regions.

In addition to her work in IP law, Manisha Singh also serves as standing Counsel for the RBI at the Delhi High Court. She possesses a strong understanding of corporate, banking and financial services laws.

Singh graduated with a Bachelor of Laws in Intellectual Property from Delhi University in 1997 and with a Master of Arts in Economics from Patna University in 1994. She completed her Economics Honours at Patna Women's College in 1992.

LexOrbis
709/710, Tolstoy House
15–17, Tolstoy Marg
New Delhi
India

Tel: +91 98 1116 1518
Email: manisha@lexorbis.com
LinkedIn: www.linkedin.com/in/manisha-singh-509b698/

Srinjoy Banerjee is a Partner at LexOrbis, leading the Privacy and Data Protection vertical. A lawyer by profession, he holds more than 23 years of experience in data protection laws, IP litigation and prosecution, policy framework and implementation, Information Technology, cyber laws and compliance and risk, among others.

Over the years, Srinjoy has transformed from a core IP professional to a privacy professional and has been extensively working on data protection laws. He is a Certified Information Privacy Professional/Europe (CIPP/E), a Certified Information Privacy Manager (CIPM) and a Fellow of Information Privacy (FIP) at the International Association of Privacy Professionals (IAPP). He has also undertaken the certification for and is a Data Security Council of India (DSCI) Certified Privacy Lead Assessor (DCPLA). He also holds an MBA in Information Technology Management from AIMA.

He has trained 600+ professionals in the field of data privacy in the IAPP certifications (CIPP/E & CIPM) and, GDPR, and enforcement agencies and enthusiasts in IP and cyber laws. He has also trained Cyber Cells (Police) of Kolkata and Bengaluru. He was a Co-Chair of the Delhi Chapter. He is also a regular speaker on data privacy at multiple national and international forums.

LexOrbis
606–607, 6th Floor, Gamma Block
Sigma Soft Tech Park, No.7 Whitefield Main Road
Varthur Hobli, Bengaluru – 560066
India

Tel: +91 80 4324 5900
Email: srinjoy.banerjee@lexorbis.com
LinkedIn: www.linkedin.com/in/srinjoybanerjee

LexOrbis is a premier full-service IP law firm with over 320 personnel, including 180+ attorneys at its five Indian offices in Ahmedabad, Bengaluru, Chennai, Mumbai and New Delhi. The firm provides client-oriented and cost-effective solutions for the protection, enforcement, transaction and commercialisation of all forms of IP in India and globally. The firm has been consistently ranked amongst the Top 5 IP firms in India over the past decade and is well known for managing global patent, designs and trademark portfolios of many technology companies and brand owners. The firm has dedicated teams to cater to the IP lifecycle, including attorneys, engineers, scientists and specialists to deal with patent, trademark and copyright filing, research, portfolio building and management, enforcement, protection, spotting, transacting, procurement and consultation.

The trademark practice group at the firm has over 40 attorneys experienced in partnering with brand owners and advising on the entire IP lifecycle from selection to enforcement. The team provides risk assessment by conducting trademark searches in over 120 trademark registers across the world and common law searches using advanced internet-based tools.

The firm's patent practice group has over 110 patent attorneys with domain expertise in information and communication technologies (ICT), computer sciences and software, including artificial intelligence/machine learning, IoT, blockchain, big data, mechanical, electrical & electronics, chemical and pharmaceutical, biotechnology, energy management, etc. The firm employs cutting-edge technology systems to improve processes and efficiency. The firm's professionals are known for their clear communication, responsiveness, quick turnaround time, and out-of-the-box thinking and solutions.

www.lexorbis.com

LexOrbis | Intellectual Property Attorneys & Advocates

iclg International Comparative Legal Guides

The **International Comparative Legal Guides** (ICLG) series brings key cross-border insights to legal practitioners worldwide, covering 58 practice areas.

Cybersecurity 2025 features two expert analysis chapters and 21 Q&A jurisdiction chapters covering key issues, including:

- Cybercrime
- Cybersecurity Laws
- Preventing Attacks
- Specific Sectors
- Corporate Governance
- Litigation
- Insurance
- Investigatory and Police Powers
- International Compliance
- Future Developments

The International Comparative Legal Guides are published by: glg Global Legal Group