



THE INSTITUTE OF  
Company Secretaries of India

भारतीय कम्पनी सचिव संस्थान

IN PURSUIT OF PROFESSIONAL EXCELLENCE

Statutory body under an Act of Parliament

(Under the jurisdiction of Ministry of Corporate Affairs)

# SUPPLEMENT PROFESSIONAL PROGRAMME

*for*  
*December, 2025 Examination*

## ARTIFICIAL INTELLIGENCE, DATA ANALYTICS AND CYBER SECURITY – LAWS & PRACTICE

### GROUP 1 ELECTIVE PAPER 4.4

*Disclaimer: This document has been prepared purely for academic purposes only and it does not necessarily reflect the views of ICSI. Any person wishing to act on the basis of this document should do so only after cross checking with the original source.*

## INDEX

<b>Lesson no.</b>	<b>Lesson Name</b>	<b>Page no.</b>
<b>1</b>	Artificial Intelligence (“AI”) – Introduction and Basics	3
<b>2</b>	Cyber Security	11
<b>3</b>	Cyber Threats and Cyber Laws	15
<b>4</b>	Cyber Crimes and Investigation Procedures	34
<b>5</b>	Regulatory Framework on AI, Cyber Security and Cyberspace	40
<b>6</b>	Data Analytics and Law	49

## Lesson 1 - Artificial Intelligence (“AI”) – Introduction and Basics

### Artificial Intelligence and Intellectual Property Rights

Introduction of Artificial Intelligence and its use has considerably changed the arrangement of how people work. Similarly, its use in intellectual property has become increasingly prevalent. One of the most important applications of AI in IP is the creation of new work as it can generate original work. AI focuses on performing tasks with the help of intelligence methods such as Reasoning, Machine Learning, Problem Solving, Perception, and Linguistic Intelligence. With the help of AI-powered algorithms, comprehensive searches of existing IP databases can be performed more efficiently and accurately. Along with this, it also helps in analyzing technical information and documents to determine existing relevant work to prevent copyright infringement. As AI technology becomes more advanced, it will likely be used more in areas related to intellectual property. This could lead to new legal issues and problems.<sup>1</sup>

“As artificial intelligence (AI) continues to emerge as a general-purpose technology with widespread applications throughout the economy and society, this poses fundamental questions that sit at the heart of the existing IP systems. Some major questions involve – (i) Does AI innovation and creation need IP incentives? (ii) How should the value of human invention and creation be balanced against AI innovation and creation? (iii) Does the advent of AI require any changes to the existing IP frameworks?” - **World Intellectual Property Organization**

Some of the IPR issues related to AI generated output are as follows:

#### 1. Ownership and Authorship

One of the most important legal challenges posed by Artificial Intelligence on IP is the issue of ownership and authorship of AI-generated works. As discussed earlier, one can generate original work with a high level of creativity with the help of AI but the question arises ‘Who owns that work?’ one who gives directions to the AI system to create the work (User), the developer of the AI system, or the AI system itself. According to the traditional intellectual property law, the creator or author of the work is considered the sole owner of the work but this is not the case with the AI-generated art.

#### 2. Copyright Challenges

The ability of Artificial Intelligence to generate huge content quickly raises copyright issues as it can easily duplicate and reproduce copyrighted content such as images, texts, videos, music, etc. AI-powered systems can copy any work or art or content without permission of the owner, making it difficult to identify the original and duplicate or unauthorized work. Now, the question arises whether the content generated through AI can be copyrighted. In most jurisdictions including Spain and Germany, it has been determined that only works created by a human being can be protected by copyright.

A key question regarding AI copyright in India is whether computer-authored works meet the originality criterion under Section 13 of the Copyright Act<sup>2</sup>. Courts have interpreted originality as intellectual effort furnished by humans. But training neural networks involves significant human endeavour in curating datasets, designing architectures, etc. Developers argue this effort imbues originality into works like AI-

<sup>1</sup> Reproduced from Impact of AI on Intellectual Property Practices (January 31, 2024), Free Law.

<sup>2</sup> The Copyright Act, 1957, §13, No. 14, Acts of Parliament, 1957 (India)

generated music<sup>3</sup>. Similarly, in the M/S Kibow case, the Delhi High Court ruled that AI systems cannot be officially registered as the proprietor of a trademark. It also highlighted that the Trade Marks Act, of 1999 illustrates that only a human being can apply for and be officially registered as the proprietor of a trademark.

Amending the law to designate AI developers as owners could incentivize building socially useful AI assistants and content generators. However, some caution this may create monopolies over data used to train models.<sup>4</sup> Nuanced provisions may be needed to balance interests, like compulsory licensing of protected AI works. Infusing human intent into generative processes can also strengthen copyright claims. India's jurisprudence around AI copyright will likely evolve case-by-case.

However, others contend processing data alone may not satisfy originality – focus should be on the creative process itself.<sup>5</sup> Especially with advanced AI like Generative Adversarial Networks, outputs manifest autonomously with little human input during generation. Even if AI works get copyright, determining the rights-holder is difficult – the programmer, user, or AI system itself? Overall, more clarity is required on copyright's applicability to AI works in India.

### **3. Patent Law**

India's patent regime faces similar quandaries around AI. Under Section 2(1) of the Patents Act<sup>6</sup>, AI developed inventions like new chemicals or devices may meet patentability criteria of novelty, utility and industrial applicability. However, such works may not demonstrate sufficient inventive step since the AI system rather than a human brain conceived the invention<sup>16</sup>. This could preclude patentability.

Again, developers try asserting their efforts training the model should count<sup>17</sup>. But others argue the critical inventive aspect under law is conceiving the final patented product or process, which AI does autonomously.<sup>7</sup> Section 6's terminology of identifying a human "true and first inventor" also suggests difficulty accommodating AI inventors.<sup>8</sup> Like copyright, approaches are debated like designating the programmer or user as deemed inventor for AI creations.

Clearer guidelines are required on evaluating and assigning patents for AI outputs. Suitably defining inventiveness for AI systems, while upholding patent law's intent of protecting true human inventors, will be key. India could emulate US and UK patent office moves to allow naming AI systems alongside humans as joint applicants on patents they contributed to<sup>21</sup>. Overall, India's patent law will require modernizing to appropriately incentivize AI innovation.

### **4. Other IPR Issues**

Automated content generation, data privacy and security, deep fakes, and manipulated content are some other issues posed by AI in safeguarding intellectual rights. Moreover, the use of AI increases various

---

<sup>3</sup> Ramakrishna B & Anil Kumar H.S., Fundamentals of Intellectual Property Rights: For Students, Industrialist and Patent Lawyers (2017)

<sup>4</sup> Ibid

<sup>5</sup> Guadamuz, A. (2021). Do androids dream of electric copyright? Comparative analysis of originality in artificial intelligence generated works. Intellectual Property Quarterly, (2), 169-186

<sup>6</sup> The Patents Act, 1970, §2(1), No. 39, Acts of Parliament, 1970 (India)

<sup>7</sup> Yanisky-Ravid, S., & Liu, X. (2018). When artificial intelligence systems produce inventions: An alternative model for patent law at the 3A era. Mich. St. L. Rev., 2018, 839

<sup>8</sup> The Patents Act, 1970, §6, No. 39, Acts of Parliament, 1970 (India)

ethical concerns; therefore, there is a need to balance the benefits of AI with the protection of intellectual property rights by introducing appropriate frameworks.

### **Requirement of Amendment in Laws**

Due to the emergence of AI, below are some of the sections that may require changes in the IPR related laws<sup>9</sup>

- **Copyright:** AI-generated works may raise questions about authorship and ownership. Section 17 of the Copyright Act may need to be amended to address the issue of ownership of AI-generated works.
- **Patents:** AI technology can generate novel inventions that may require patent protection. Section 3(k) of the Patents Act may need to be reviewed to address the patentability of AI-generated inventions.
- **Trademarks:** AI systems can generate trademarks, which raises questions about the ownership and distinctiveness of such marks. Sections 9 and 11 of the Trademarks Act may require amendments to address these issues.
- **Trade secrets:** AI technology can facilitate the disclosure and misappropriation of trade secrets. Section 2(1)(a) of the Trade Secrets Act may need to be amended to clarify what constitutes a trade secret in the context of AI.
- **Enforcement:** The use of AI can make it difficult to detect and enforce IPR violations. Section 53 of the IPR Act may need to be amended to address these challenges and to ensure that appropriate enforcement mechanisms are in place.

### **Existing IPR regime well-equipped to protect AI generated works, no need to create separate category of rights<sup>10</sup>: Recent Statement of Union Minister of State for Commerce and Industry, Government of India in a written reply in the Rajya Sabha on 9<sup>th</sup> February,**

Intellectual Property Rights including Copyright and Related rights provide exclusive rights to the right owner who are legal persons for a set duration. These rights allow for the work or creation or innovation to be protected and enables collection of royalties through licensing. For a right to be granted, the owner is required to meet the criteria specified under the law. India being a member of all major international conventions and agreements for the protection of Intellectual Property Rights grants adequate protection of rights for works created by legal persons through Copyright Law and protects inventions through the Patent system. Therefore, there is no requirement to create a separate category of rights for AI and related innovations in the Indian IPR Regime. Therefore, while Artificial Intelligence (AI) and related innovations is an evolving stream of technology the current legal framework under the Patent and Copyright Act is well-equipped to protect Artificial Intelligence generated works and related innovations. Presently, there is no proposal to create any separate right so ram end the law in the context of AI-generated content.

The exclusive economic rights of a copyright owner such as the right of reproduction, translation, adaptation etc. granted by the Copyright Act, 1957 obligates the user of Generative AI to obtain permission to use their works for commercial purposes if such use is not covered under the fair dealing exceptions provided under Section 52 of the Copyright Act. Since Intellectual property rights are private rights, these are enforced by the individual rights holders. Adequate and effective civil measures and criminal remedies are prescribed under the Copyright Law against any act of infringement or unauthorized use of works,

---

<sup>9</sup> Reproduced from Vishaka Aditya, Navigating the Legal Challenges posed by AI on Intellectual Property, Legal Service India

<sup>10</sup> This information has been provided by the Union Minister of State for Commerce and Industry, Shri. Som Parkash in a written reply in the Rajya Sabha on 9<sup>th</sup> February, 2024. Reproduced from Press information Bureau. Available at <https://pib.gov.in/PressReleasePage.aspx?PRID=2004715>

including digital circumvention.

### **Recent Indian Case Laws Related to AI and Intellectual Property<sup>11</sup>:**

AI technology has had an impact on landmark judgments passed by the courts in India.

These case laws demonstrate the need for clarity and amendments in Indian intellectual property laws to address the emerging challenges posed by AI technology. The Indian judiciary has taken a pragmatic approach in these cases by balancing the need for innovation with the protection of intellectual property rights.

These case laws demonstrate the evolving nature of the relationship between AI and intellectual property in the Indian legal system and highlight the need for clear legal frameworks to address the legal challenges posed by AI on intellectual property.

In 2021, the Delhi High Court ruled in the case of *M/S Kibow Biotech vs. M/S The Registrar of Trade Marks* that an AI system cannot be considered a proprietor of a trademark. The court held that under the Trade Marks Act, of 1999, only a person can apply for and be registered as the proprietor of a trademark, and an AI system cannot be considered a person for the purposes of the Act.

In another case, *Ferid Allani v. Union of India*, the Delhi High Court examined the issue of whether an AI-generated work can be copyrighted in India. The court held that copyright protection can be granted to AI-generated works if they meet the criteria for originality and authorship under the Copyright Act, of 1957. The court also held that the authorship of an AI-generated work should be attributed to the person who decided to create the work, such as the programmer or user of the AI system.

In the case of *South Asia FM Limited v. Union of India*, the Delhi High Court examined the issue of whether a song created by an AI system could be considered a work of original authorship under the Copyright Act, of 1957. The court held that the song was not eligible for copyright protection as it lacked the human element of creativity and was the result of an algorithmic process. The court held that for a work to be eligible for copyright protection, it must result from human creativity and originality.

In the case of *Gaurav Bhatia v. Union of India*, the Delhi High Court held that AI-generated inventions could be patented if they met the requirements of novelty, non-obviousness, and industrial applicability under the Patents Act.

In the case of *Nippon Steel Corporation v. Union of India*, the Bombay High Court held that computer programs that generate inventions or discoveries could not be patented because they are not capable of being invented by a person.

In the case of *In Re: Sugan Life Sciences Pvt. Ltd*, the Indian Patent Office rejected a patent application for a drug discovery algorithm, stating that it was not a patentable invention under Section 3(k) of the Patents Act because it was a computer program per se.

---

<sup>11</sup> Reproduced from Vishaka Aditya, Navigating the Legal Challenges posed by AI on Intellectual Property, Legal Service India

In the case of Dr. Alaka Sharma v. Union of India, the Delhi High Court held that an AI-generated portrait could not be registered as a trademark under the Trademarks Act because it did not satisfy the distinctiveness requirement.

In the case of MySpace Inc. v. Super Cassettes Industries Ltd., the Delhi High Court held that an AI-based algorithm used to identify and remove infringing content on a social media platform did not violate the Copyright Act because it was not reproducing the copyrighted content.

### **Steps of Government of India on Artificial Intelligence: A Snap Shot<sup>12</sup>**

As per the information given by the Minister of State for Electronics & Information Technology, in a written reply to a question in Lok Sabha on Government of India has taken several steps to promote upskilling or reskilling in the field of Artificial Intelligence which include the following: -

Ministry of Electronics and IT (MeitY) has initiated a programme titled FutureSkills PRIME ([www.futureskillsprime.in](http://www.futureskillsprime.in)) in collaboration with NASSCOM, a B2C framework for re-skilling/ up-skilling of IT professionals in 10 Emerging areas including Artificial Intelligence. So far, 7 Lakh candidates have signed-up on the FutureSkills PRIME Portal, out of which, 1.2 lakh candidates have completed their courses. In addition, 524 Trainers and 4292 Government Officials have been trained on these technologies by NIELIT/C-DAC Resource Centres, and around 1.3 lakh unique learners have collectively earned 8.9 lakh 'badges' in recognition of having completed bite-sized digital fluency content. Under Artificial Intelligence, 36,528 candidates are enrolled in deep – skilling courses and 47,744 candidates are enrolled in Foundation courses.

Government has published the National Strategy for Artificial Intelligence in June 2018 and proposes to develop an ecosystem for the research and adoption of Artificial Intelligence i.e. #AIFOR ALL. Government has launched 'National AI Portal' (<https://indiaai.gov.in/>) which is a repository of Artificial Intelligence (AI) based initiatives in the country at a single place. As on date, there are 1024 national and international articles, 655 news, 200 videos, 90 research reports, 279 Startups, 120 Government initiatives listed at National AI Portal.

In addition, various steps have been taken to promote capacity building in Artificial Intelligence which include the following:

Government has initiated 'Visvesvaraya PhD Scheme' with an objective to enhance the number of PhDs in Electronics System Design & Manufacturing (ESDM) and IT/IT Enabled Services (IT/ITES) sectors in the country. The research areas under the scheme include Artificial Intelligence (covering 82 PhD fellows) and Machine Learning (covering 59 PhD fellows).

National Programme on Responsible Use of AI for Youth: With the objective to empower the youth to become AI ready and help reduce the skill gap, government along with Industry partner has started this initiative to promote AI awareness among Government school going children. In Phase I, 50,666 students and 2536 teachers from 2252 schools from 35 States and UTs attended orientation sessions on AI. In Phase II, 100 teams have been short listed and have undergone extensive mentoring by AI experts. In Phase-III, Top 20 students have demonstrated their solutions in the national conference.

---

<sup>12</sup> Reproduced from Artificial Intelligence, published by Press Information Bureau of India. Available at <https://www.pib.gov.in/PressReleasePage.aspx?PRID=1811372>

To foster innovation through research, government has created several ‘Centres of Excellence’ on various Emerging Technologies including Artificial Intelligence. These centres connect various entities such as startups, enterprises, venture capitalists, government and academia to look into problem statements and develop innovative solutions.

Department of Science & Technology is implementing the National Mission on Interdisciplinary Cyber-Physical Systems (NM-ICPS) to promote R&D, Human Resource Development (HRD), Technology Development, Entrepreneurship Development, International Collaboration etc. As part of the Mission implementation, 25 Technology Innovation Hubs (this) have been established in reputed institutes across the country in advanced technologies including Machine Learning and Artificial Intelligence.

Government of India has also joined the league of leading economies including USA, UK, EU, Australia, Canada, France, Germany, Italy, Japan, Mexico, New Zealand, Republic of Korea, Singapore as a founding member of the Global Partnership on Artificial Intelligence (GPAI), which is an international and multi-stakeholder initiative to guide the responsible development and use of AI, grounded in human rights, inclusion, diversity, innovation, and economic growth.

Government of India organized Responsible AI for Social Empowerment (RAISE) in 2020, a first-of-its-kind global meeting of minds on Artificial Intelligence to drive India’s vision and roadmap for social transformation, inclusion and empowerment through responsible AI. It was attended by 79,000+ stakeholders from academia, research, industry and government representatives from 147 participating countries. 320 distinguished speakers from 21 countries participated in the event.

The initiatives mentioned above are focusing on digital enablement of citizens in the field of Artificial Intelligence including those belonging to the Tier 2 & Tier 3 cities. Further, the Future Skills PRIME programme follows an ‘aggregator of aggregators’ approach for digital skills training on a national scale and is hosted as an online B2C-commerce platform, thereby also enabling citizens in Tier 2 & Tier 3 cities to participate in the programme. To further strengthen the physical and digital connectivity, 40 C-DAC/NIELIT Centres spread across the country are also institutionalizing blended-learning programmes, in a hub and spoke mode, as Lead & Co-Lead Resource Centres.

Further, the Future Skills PRIME programme targets to re-skill/ up-skill aspirants in emerging technologies so that they stay relevant in their present job with improved prospects, besides finding new avenues in future job-roles. The programme also targets those who may have lost their existing jobs due to disruptive and emerging technologies. Towards this, the programme takes into account employment linkages, such as a ‘Career Prime’ web-page on the platform and an integrated ‘Career Portal’, which provides information on IT-ITeS jobs, internships, apprenticeships, hackathons etc.

Under Future Skills PRIME, incentives are available to the trainees, including those from economically weaker backgrounds, after the learner is successfully assessed and certified. The incentive mechanism is aimed at motivating the learner to successfully complete the online up- skilling/re-skilling programs.

### **AI Preparedness Index (AIPD)<sup>13,14</sup>**

**AI Preparedness Index (AIPD)** assesses the level of AI preparedness across 174 countries, based on a rich set of macro-structural indicators that cover the countries’ digital infrastructure, human capital and labor market policies, innovation and economic integration, and regulation and ethics.

Source data include official data, surveys of hard data and surveys of perceptions compiled by 8 institutions: Fraser Institute, International Labor Organization, International Telecommunication Union, United

Nations, United Nations Conference on Trade and Development, Universal Postal Union, World Bank, and World Economic Forum.

As described in the index documentation and the published paper, the AIFI is the sum of four key dimensions: digital infrastructure, human capital, technological innovation, and legal frameworks. These four dimensions are likely relevant for smooth AI adoption. In turn, each dimension is computed by normalizing and averaging a rich set of sub-indicators including, but not limited to, the presence of relevant digital infrastructure, sustained human capital investment, inclusive STEM expertise, labor and capital mobility, a vibrant R&D ecosystem, and the adaptability of legal frameworks to digital business models.

### **How to use the AIFI:**

1. Be aware that the index incorporates several perceptions-based indicators, reflecting individuals' subjective assessments and experiences. Therefore, the index should be seen as an indicative measure, guiding policymakers in identifying areas for improvement rather than being used for ranking purposes.
2. Note that the focus is on AI adoption preparedness (rather than on invention leadership), which allows for comparability of the level of preparedness across all economies.
3. Recognize that measuring AI preparedness is challenging because the institutional requirements for economy-wide integration of AI are still uncertain.

---

<sup>13</sup> <https://www.imf.org/external/datamapper/datasets/AIFI>

<sup>14</sup> <https://www.imf.org/external/datamapper/AIFINote.pdf>

## Lesson 2- Cyber Security

### National Cyber Security Strategy 2023: Latest Updates<sup>15</sup>

Lt. Gen. Rajesh Pant (retd.), national cyber security coordinator, National Security Council Secretariat, said that the National Cyber Security Strategy 2023 is in final stages of approvals.

National Cyber Security Strategy 2023 is an important document that supersedes the 2013 policy. From 2013 till 2023, the world has changed as new threats have emerged calling for new strategy.

The government has been consistently working on providing structured guidance on cyber security to critical sectors of the nation which include telecom, power and energy, transportation, finance, strategic entities, government entities and health. This major initiative is driven by the National Critical Information Infrastructure Protection Centre under a project funded by the National Security Council Secretariat.

Organizations can use the NCRF to improve their cybersecurity posture, reduce data breach risk or any cybersecurity incident, ensure compliance with regulations and enhance operational efficiency.

The official said that the Centre has spent ₹700 crore on national cyber awareness and cyber skilling programme initiative.

There are two aspects to cyber security. First is cyber hygiene for all of us and cyber skilling of the cyber workforce i.e. the people who enforce cyber security. For the first part we have a programme ISEA (Information Security Education and Awareness) programme which is now in phase II, implemented by the ministry of electronics and IT and CDAC, Hyderabad is the nominated agency for spreading public awareness. Cyber skilling is another programme run in government and private universities where syllabus has changed as per the changing needs. I agree that a lot more needs to be done.

### Bharat National Cyber Security Exercise 2023: Elevating India's Cybersecurity Preparedness to New Heights<sup>16</sup>

The prestigious SCOPE Convention Centre in New Delhi bore witness to the Bharat National Cyber Security Exercise (NCX) 2023, an event of monumental significance spanning from October 9th to 20th October 2023. This momentous occasion is a remarkable milestone in India's unwavering quest for cybersecurity excellence.

This flagship event served as a unifying platform for over 300 participants, representing a diverse spectrum of government agencies, public organizations, and the private sector, all resolutely committed to the safeguarding of critical information infrastructure.

Organized by the National Security Council Secretariat (NSCS), Government of India (GoI), in strategic partnership with Rashtriya Raksha University (RRU), Bharat NCX 2023, has been stressed upon the importance of cyber security in today's world and mentioned that future battle will be fought primarily in

---

<sup>15</sup> Reproduced from Inamdar Nadeem (June 13, 2023), National Cyber Security Strategy 2023 to be released soon, The Hindustan Times. Available at <https://www.hindustantimes.com/cities/pune-news/sena-ubt-firm-on-contesting-sangli-seat-101712345210167.html>

<sup>16</sup> Reproduced from Bharat National Cyber Security Exercise 2023 Concludes: Elevating India's Cybersecurity Preparedness to New Heights (October 23, 2023), Press Information Bureau of India. <https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1970225#:~:text=Bharat%20NCX%202023%20while%20making,and%20enhancing%20Public%20Private%20Partnership>.

the cyber domain. Experts also stressed on the importance of operational technology in the domain of cyberspace.

Bharat NCX 2023 represents a defining moment in India's unwavering commitment to cybersecurity excellence, underscoring the paramount importance of collaboration and knowledge-sharing among stakeholders from government, public, and private sectors.

Bharat NCX 2023, organised intense training for the participants over six days and a red on blue Live Fire cyber exercise over five days, wherein participants challenged their cyber skills against a determined adversary. The exercise also had a Strategic Track for leadership level discussions on cyber threat landscape, incident response, crisis management to handle real world cyber challenges.

Bharat NCX 2023 while making endeavours to fortify our cyber defences also highlighted the need for a National Cyber Security Strategy resulting in governance structures supported by legal frameworks, efficient processes for threat intel sharing and enhancing Public Private Partnership.

In an era characterized by burgeoning digitalization, Bharat NCX 2023 serves as a compelling reminder of the paramount importance of collective vigilance and preparedness in safeguarding our nation's invaluable digital assets.

### **Digital Personal Data Protection Act, 2023: New Paradigm of Data Privacy and Compliance<sup>17</sup>**

After receiving approval from both houses of Parliament and obtaining the President's assent, the Digital Personal Data Protection Bill of 2022 has officially become the Digital Personal Data Protection Act of 2023. This Act is now in effect and governs the processing of digital personal data in India, regardless of whether the data was originally collected in digital or non-digital format and subsequently digitized. Under the DPDP Act, state agencies may be exempted from its provisions at the government's discretion. This legislation is designed to bolster data protection and accountability for entities such as internet companies, mobile apps, and businesses that handle citizens' data. Furthermore, it's worth noting that the DPDP Act will have implications for India's trade negotiations with other nations. It aligns with global data protection standards, taking inspiration from models like the EU's GDPR and China's PIPL.

At its core, the DPDP Act aims to establish a higher level of accountability and responsibility for entities operating within India, including internet companies, mobile apps, and businesses involved in the collection, storage, and processing of citizens' data. With a strong emphasis on the "Right to Privacy," this legislation seeks to ensure that these entities operate transparently and are answerable when it comes to handling personal data, thus prioritizing the privacy and data protection rights of Indian citizens.

The DPDP Act's scope extends beyond the borders of India, encompassing digital personal data processing activities abroad. This extension applies specifically to organizations offering goods or services to individuals in India or engaging in the profiling of Indian citizens. In doing so, the Act fortifies data protection measures not only within India but also concerning Indian citizens' data handled abroad.

---

<sup>17</sup> Reproduced from Khyati Anand and Melissa Cyrill (September 18, 2023), India's Digital Personal Data Protection Act, 2023: Data Privacy Compliance India Briefing. Available at <https://www.india-briefing.com/news/indias-digital-personal-data-protection-act-2023-key-provisions-29021.html/>

## **The Telecommunications Act, 2023: Added Leg in Cyber Security**

The Telecommunications Act, 2023 amended and consolidated the laws relating to development, expansion and operation of telecommunication services and telecommunication networks; assignment of spectrum; and for matters connected therewith or incidental thereto.

### ***Lawful Interception and Security***<sup>18</sup>

The Telegraph Laws empowered Government to intercept messages under a mechanism, which has survived judicial review for decades<sup>19</sup>, and inspired similar regimes<sup>20</sup>. Interception directions are required to be in writing, on specified grounds and are subject to review by a committee<sup>21</sup>.

The Telecommunications Act, 2023 contains provisions empowering Government to take possession of Services or networks and direct interception or disclosure of messages, in the event of a public emergency or in the interest of safety, with measures to be specified in rulemaking. To the extent that existing safeguards flow through to the new regime, especially given that right is couched in “public safety”, it should continue to provide a robust and constitutional basis for lawful interception and monitoring.

The Act introduces ‘critical telecommunication infrastructure’, along the lines of ‘critical information infrastructure’ under the Information Technology Act, 2000 (“IT Act”).<sup>22</sup> Regulations in relation to the protection of critical telecommunications infrastructure will be prescribed under the rules.

The Government’s power to notify standards, which were introduced in the Bill, have been:

- modified to notify standards and conformity assessment measures for services in consonance with relevant TRAI regulations; and
- expanded to include prescription of standards for telecommunication security, including identification, analysis and prevention of intrusion in services and networks, cyber security and encryption and data processing in telecommunication.

These powers may impact entities not falling within the contours of the Act through contractual flow-down obligations in their capacity as service providers.

Appointments to TRAI have been broad based to enable appointments from the private sector.

## **Cyber Governance Code of Practice United Kingdom**<sup>23</sup>

The Cyber Governance Code of Practice (the Code) has been created to support boards and directors in governing cyber security risks. The Code sets out the most critical governance actions that directors are responsible for.

The Code forms part of the government’s free package of support on cyber governance and should be the first point of reference for board members. It is underpinned by Cyber Governance Training, which helps boards and directors to strengthen their understanding of how to govern cyber security risks, and the Cyber Security Toolkit for Boards, which supports boards and directors in implementing the actions set out in the Code.

- The Cyber Governance Code of Practice sets out what action’s boards need to take.
- The Cyber Governance Training confirms why and how board members take those actions.
- The Cyber Security Toolkit for Boards underpins the two, further supporting directors and board members.

The Cyber Governance Code of Practice is tailor-made for boards and directors of both public-sector and private organisations. The Code is not intended to be used by those who are responsible for the day-to-day management of cyber security, but can be used to highlight to boards what their responsibilities are. The Code has been designed for medium and large organisations. However, whilst it has not been specifically created for small organisations, they play a critical role in the resilience of the U K economy

and should seek to implement the Code's principles. Small organisations should also refer to the NCS C website (<https://www.ncsc.gov.uk/section/advice-guidance/small-medium-sized-organisations>) for further guidance that is designed for them.

---

<sup>18</sup> Reproduced from Arun Prabhu, Anirban Mohapatra & Anoushka Soni (January 23, 2024) The Telecommunications Act, 2023, Indian Corporate Law, Cyril Amarchand Mangaldas. Available at <https://corporate.cyrilamarchandblogs.com/2024/01/the-indian-telecommunications-bill-2023/#:~:text=Lawful%20Interception%20and%20Security&text=The%20Act%20contains%20provisions%20empowering,to%20be%20specified%20in%20rulemaking>.

<sup>19</sup> People's Union of Civil Liberties v. Union of India, (2003) 2 SCR 1136

<sup>20</sup> The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Rule 4(2)

<sup>21</sup> Indian Telegraph Rules, 1951, Rule 419A(2)

<sup>22</sup> Information Technology Act, 2000, Section 70

<sup>23</sup> [https://assets.publishing.service.gov.uk/media/67ffbb23b73354468d135555/Cyber\\_Governance\\_Code\\_of\\_Practice\\_-\\_web\\_accessible.pdf](https://assets.publishing.service.gov.uk/media/67ffbb23b73354468d135555/Cyber_Governance_Code_of_Practice_-_web_accessible.pdf)

## Lesson 3 – Cyber Threats and Cyber Laws

### Digital India Act - An Act in Progress to replace Information Technology Act, 2000

With digital transformation at its high in India, March 2023 has witnessed a magnificent move with the official announcement of enacting Digital India Act (DIA) while replacing a 24-year-old Information Technology Act of 2000 (IT Act). This proactive move by the Ministry of Electronics and Information Technology (MeitY) aligns with India's ambitious “Digital India” initiative.

On 9th March 2023, the Minister of State for the Ministry of Electronics and Information Technology (MeitY), held a consultation to officially announce that the Information Technology Act of 2000 (IT Act) will be replaced with a new Digital India Act (DIA), a future-ready legislation. The contents of the new act were laid down in the presentation. The MeitY is conducting rounds of consultations in the coming months and soliciting feedback from various stakeholders. This draft has generated debates and discussions on the regulation of the Internet today.<sup>24</sup>

#### Nine Pillars of Digital India

1. Broadband Highways
2. Universal Access to Mobile Connectivity
3. Public Internet Access Programme
4. e-Governance: Reforming Government through Technology
5. e-Kranti - Electronic Delivery of Services
6. Information for All
7. Electronics Manufacturing
8. IT for Jobs
9. Early Harvest Programmes

#### Necessity for Digital India Act (DIA)

The proposed Digital India Act (DIA) *inter-alia* with an aim to provide a *future ready legislation* opts “*principles and rule-based approach*” for regulating digital transactions including the evolving era of Artificial Intelligence and Machine Learning. With this background, we aim to discuss the salient features of DIA and its possible impact on industries for aligning their compliance calendar with principle and rule-based approach.

#### Need for Digital India Act

- **Outdated Regulations:** The existing IT Act of 2000 was crafted in an era when the internet had only 5.5 million users, and is ill-equipped to handle the internet's current state.
- Today, with 850 million users, various intermediaries, and new forms of user harms like cyberstalking and doxing, the IT Act falls short of addressing these complexities.
- **Inadequacy of Current Regulations:** Despite the existence of regulatory elements like Intermediary Guidelines, Digital Media Ethics Code, and data protection rules, they are insufficient when it comes

<sup>24</sup> Reproduced from Sanhita Chaurita (8<sup>th</sup> August 2023) Explained: The Digital India Act 2023, Vidhi Centre For Legal Policy.

to governing new-age technologies.

- **Need for Legal Adaptation:** With technological advancements like AI, Blockchain, and IoT, the legal framework must evolve to address their unique challenges. This includes enhancing cybersecurity measures, data protection, and regulating emerging tech sectors.
- **Addressing E-commerce and Online Content:** The growth of e-commerce, digital transactions, and online content sharing requires updated regulations. The Digital India Act will tackle issues related to consumer protection, electronic contracts, and content moderation on social media platforms.
- **Global Alignment and Best Practices:** To engage effectively in the global digital landscape, India's regulations must align with international standards and practices.

On the path of digital economy, we are already witnessing reformative landscape of legal and regulatory regime with major focus on fintech sectors, enterprise and deep technology sectors, e-commerce, consumer protection and data management.

Among other factors, following the major reasons which necessitates the introduction of proposed Digital India Act:

Limitation of IT Act, 2000	Challenges in Cyberspace	Tech-Aligned Regulation
<ul style="list-style-type: none"> <li>• IT Act is around 24 years old and was enacted in early days of internet.</li> <li>• It does not adequately cover modern internet-based services such e-commerce, social media platforms and alike.</li> <li>• Inadequate principles for data / privacy protection.</li> <li>• Legal recognition of electronic records, transactions and electronic signatures over the electronic medium.</li> </ul>	<ul style="list-style-type: none"> <li>• Multiple categories of Intermediaries.</li> <li>• Digital Media</li> <li>• Social Media</li> <li>• AI and ML</li> <li>• OTT</li> <li>• Complex forms of user harms – sim-swaps, catfishing, cyber stalking, online gaslighting.</li> <li>• Disinformation.</li> <li>• Increased flow of data and need to regulate the data at global parameters.</li> <li>• Alignment with contemporary regulations including DPDP Act, 2023 and Limitation Act, 1963.</li> </ul>	<ul style="list-style-type: none"> <li>• Need for Global Standards of Cyber Laws</li> <li>• Comprehensive need on user rights, trust &amp; safety.</li> <li>• Emerging Technology.</li> <li>• High risk automated-decision making systems.</li> <li>• New forms of cybercrimes.</li> <li>• Requirement of a converged, coordinated &amp; harmonized institutional regulatory body.</li> <li>• To strengthen user rights and security specially women and child safety.</li> </ul>

The proposed DIA includes following salient features:

- Principle and Rule based Approach
- Digital Governance and Adjudicatory Architecture
- Open Internet
- Safe and Secure Cyberspace
  - *For example - strengthening the penalty framework for non-compliance and issuing advisories on the information & data security practices, etc.*
- Responsible and Ethical Use of Online Technologies
- Safeguard Innovation and Promoting Start-ups

- Digital User Rights
- Regulation of Intermediaries (basis the type of Intermediary) –
  - For example, enterprise software providers such as cloud service providers should not be subjected to the same set of regulations as that of significant social media intermediaries.
- *Principle of Safe Harbour*
  - Accountability
  - Inclusive Regulatory Framework – *Balanced with sectoral regulations.*
  - Emerging Technology, Risk (Management) and Guard Rails
  - Ensuring Safety and Privacy of Children (*Industry Specific Requirements*)
  - Algorithmic Transparency and regulation of Artificial Intelligence (“AI”)

### **Requirement of Industry Alignment towards Goals and Proposed Structure of DIA:**

One shall always remember one of powerful legal maxim “*Ignorantia Juris Non Excusat*”, which means ignorance of law is not an excuse. Hence, one should stay prepared before the proposed DIA is notified. It is to be noted that separate rules will govern different kinds of industry. Hence ***Industry Specific Compliance Calendars*** will be required. Although pursuant to notification of DIA, a detailed proposal on the requirements under DIA along with strategy and pedagogy on compliance calendars shall follow.

### **Challenges Ahead in the Implementation of DIA, 2023<sup>25</sup>**

- **Burdensome Compliance Requirements:** The act’s regulations may place a significant burden on businesses, particularly small and medium-sized enterprises (SMEs).
- **Freedom of Expression:** The review of the "safe harbor" principle for online platforms could potentially impact freedom of expression. Ensuring that the act doesn't curb this fundamental right is a delicate task.
- **Resource and Infrastructure Requirements:** Effective enforcement of the DIA will require substantial resources, expertise, and infrastructure. Investing in these areas will be crucial.
- **Stakeholder Interests:** Balancing the interests of various stakeholders, including tech giants and citizens' rights, poses a significant challenge. Ensuring that all voices are heard and considered in the implementation process is essential.
- **Surveillance and Privacy Concerns:** Critics argue that certain provisions of the act may grant excessive surveillance powers to the government, potentially compromising privacy rights. Robust safeguards should be incorporated to protect against abuse of power and violations of privacy.
- **Data Localization and Cross-Border Data Flows:** The act’s approach to data localization is a point of contention. While localization can enhance data protection and security, it may also disrupt cross-border data flows, impacting global businesses that rely on efficient data transfers.

### **Way Forward for Effective Implementation of DIA, 2023<sup>26</sup>**

- **Stakeholder Engagement:** All relevant stakeholders, including government bodies, technology companies, legal experts, and civil society, should be involved in the drafting and implementation process. This will help create a balanced and comprehensive legal framework.

---

<sup>25</sup> Reproduced from India’s Digital Future: The Digital India Act 2023, Drishti IAS, 2023

<sup>26</sup> Reproduced from India’s Digital Future: The Digital India Act 2023, Drishti IAS, 2023

- **Balancing Regulation and Innovation:** Stricter regulations, particularly in emerging technologies, could inadvertently stifle entrepreneurial initiatives and deter foreign investments. Striking the right balance between regulation and innovation is critical.
- **Collaboration and Capacity Building:** Invest in building the capacity of law enforcement agencies, judiciary, and regulatory bodies to effectively enforce the DIA.
- Collaborate with other countries and international organizations to align the DIA with global best practices and standards in the digital space.
- **Public Awareness:** Conduct public awareness campaigns to educate citizens about their rights and responsibilities in the digital realm, fostering a culture of digital literacy.

### Way Forward<sup>27</sup>

The intention behind the DIA is laudable and this legislation will be revamping India's technology sector regulations. It is for the first time that consultations are taking place during the pre-draft stage of the bill. Policymakers are aware of the challenges that might arise therefore the opinions of important stakeholders are being valued. The need for comprehensive and relevant legislation was much needed for the evolving technology sector in India.

While the DIA will promote the growth of India's digital economy, and address the challenges which new-age technologies bring with them like data privacy and cyber security. However, doing away with the safe harbour principle will be criticized by Bigtechs. Additionally, it will require specialists and developed infrastructure for law enforcement, tackling the uncertainties of new-age technologies, AI, deep fakes, and dispute resolution in the proposed legislation. Defining territorial jurisdiction is necessary due to the borderless nature of information and interactions over the Internet. While transparency and accountability are the founding pillars of the act it will also have to balance the interests of important stakeholders like users, big techs, government, businesses, and civil society.

Undoubtedly, it will be one of the most landmark legislations in the jurisprudence of the country as it will protect the freedom of expression and the fundamental rights of citizens on social media platforms. Along with enhancing privacy, online safety, and security, it will also safeguard citizen's data. It will foster innovation and growth of new-age technologies which will be beneficial in education, health, and administration. It will be interesting to see how building this proposed legislation plays out in the coming future.

### Bharatiya Nyaya Sanhita, 2023

The Bharatiya Nyaya Sanhita, Bharatiya Nagrik Suraksha Sanhita and the Bharatiya Sakshya Adhinyam that replaced the Indian Penal Code, 1860; Code of Criminal Procedure, 1898; and the Indian Evidence Act, 1872, respectively, received President Droupadi Murmu's assent on December 25, 2023 and came into effect from July 1, 2024,

*Some of the important provisions of Bharatiya Nyaya Sanhita, 2023 dealing with Cyber Crime are as under:*

Section 111(1) of the Bharatiya Nyaya Sanhita, 2023 deals with organised Crime. It provides that any continuing unlawful activity including kidnapping, robbery, vehicle theft, extortion, land grabbing, contract killing, economic offence, cyber-crimes, trafficking of persons, drugs, weapons or illicit goods or services, human trafficking for prostitution or ransom, by any person or a group of persons acting in concert, singly

---

<sup>27</sup> Reproduced from Sanhita Chaurita (8<sup>th</sup> August 2023) Explained: The Digital India Act 2023, Vidhi Centre for Legal Policy

or jointly, either as a member of an organised crime syndicate or on behalf of such syndicate, by use of violence, threat of violence, intimidation, coercion, or by any other unlawful means to obtain direct or indirect material benefit including a financial benefit, shall constitute organised crime.

Section 152 of the Bharatiya Nyaya Sanhita, 2023 deals with act endangering sovereignty, unity and integrity of India. It states that whoever, purposely or knowingly, by words, either spoken or written, or by signs, or by visible representation, or by electronic communication or by use of financial mean, or otherwise, excites or attempts to excite, secession or armed rebellion or subversive activities, or encourages feelings of separatist activities or endangers sovereignty or unity and integrity of India; or indulges in or commits any such act shall be punished with imprisonment for life or with imprisonment which may extend to seven years, and shall also be liable to fine.

Section 228 of the Bharatiya Nyaya Sanhita, 2023 deals with fabricating false evidence. Section 228 provides that whoever causes any circumstance to exist or makes any false entry in any book or record, or electronic record or makes any document or electronic record containing a false statement, intending that such circumstance, false entry or false statement may appear in evidence in a judicial proceeding, or in a proceeding taken by law before a public servant as such, or before an arbitrator, and that such circumstance, false entry or false statement, so appearing in evidence, may cause any person who in such proceeding is to form an opinion upon the evidence, to entertain an erroneous opinion touching any point material to the result of such proceeding is said “to fabricate false evidence”.

Section 241 of the Bharatiya Nyaya Sanhita, 2023 deals with destruction of document or electronic record to prevent its production as evidence. According to Section 241 whoever secretes or destroys any document or electronic record which he may be lawfully compelled to produce as evidence in a Court or in any proceeding lawfully held before a public servant, as such, or obliterates or renders illegible the whole or any part of such document or electronic record with the intention of preventing the same from being produced or used as evidence before such Court or public servant as aforesaid, or after he shall have been lawfully summoned or required to produce the same for that purpose, shall be punished with imprisonment of either description for a term which may extend to three years, or with fine which may extend to five thousand rupees, or with both.

### **India’s Digital Personal Data Protection Act, 2023: Key Provisions<sup>28</sup>**

Initially introduced in 2019, the Digital Personal Data Protection Act holds considerable importance as a legislative measure aimed at safeguarding individuals’ privacy rights. Its primary focus lies in regulating the collection, storage, processing, and transfer of personal data in the digital landscape. The DPDP Bill underwent 81 amendments after its initial introduction, resulting in a comprehensive overhaul to its present form.

By prioritizing privacy and security, the DPDP Act strives to create a robust framework that addresses the

---

<sup>28</sup> Reproduced from Khyati Anand and Melissa Cyrill (September 18, 2023), India’s Digital Personal Data Protection Act, 2023: Data Privacy Compliance India Briefing. Available at <https://www.india-briefing.com/news/indias-digital-personal-data-protection-act-2023-key-provisions-29021.html/>

challenges posed by data handling in the digital age. Key provisions of the DPDP Act, 2023 are as follows:

**Definitions:** Although many concepts in the DPDP Act closely resemble those found in the EU's General Data Protection Regulation (GDPR), framework, there are differences in how terminology is used.

a) **Data fiduciary:** This refers to the entity that, either independently or in collaboration with others, establishes both the purpose and the methods for processing personal data (similar to a data controller). The government can classify any data fiduciary or a specific group of data fiduciaries as 'significant data fiduciaries' (SDFs). The criteria for this classification as an SDF includes the nature of processing activities (such as the volume and sensitivity of personal data involved and the potential impact on data principals' rights) to broader societal and national concerns (such as the potential effects on India's sovereignty and integrity, electoral democracy, state security, and public order). The designation of SDF comes with heightened compliance obligations as explained below.

b) **Data processor:** This is an entity responsible for processing digital personal data on behalf of a data fiduciary.

c) **Data principal:** These are individuals whose personal data is gathered and processed (equivalent to a data subject).

d) **Consent manager:** A person registered with the Data Protection Board, who acts as a single point of contact to enable a Data Principal to give, manage, review and withdraw their consent through an accessible, transparent, and interoperable platform.

**Applicability:** The DPDP Act applies to all data, whether originally online or offline and later digitized, in India. Additionally, the Act applies to the processing of digital personal data beyond India's borders, particularly when it encompasses the provision of goods or services to individuals within the Indian territory.

*Age verification mechanisms will be necessary for all companies in India (telcos, banks, e-commerce, etc.) under the new DPDP law, per reporting from The Economic Times. The compliance requirement is not just limited to social media platforms. This is essential to record the verifiable consent of users per legal experts*

**Personal data breach:** This means any unauthorized processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access to personal data, that compromises the confidentiality, integrity, or availability of personal data.

**Individual consent to use data and data principal rights:** Under the new legislation, personal data will be included and processed only with explicit consent from the individual, unless specific circumstances pertaining to national security, law, and order require otherwise. Under data principal rights, individuals also have the right to information, right to correction and erasure, right to grievance redressal, and right to nominate any other person to exercise these rights in the event of the individual's death or incapacity. Currently, there is no specified timeline for the implementation of grievance redressal and data principal rights.

**Additional obligations of SDFs:** Depending on the quantity and sensitivity of the data they manage—data fiduciaries deemed as SDF are subject to additional obligations under the DPDP Act. Every significant data fiduciary is required to appoint a Data Protection Officer (DPO) responsible for addressing the inquiries and concerns of data principals—those individuals whose data is collected and processed. Regarding international data transfers, the DPDP Act permits data fiduciaries to transfer personal data for processing to any country or territory outside India. However, the central government can impose restrictions through notifications. These restrictions will be determined after assessing relevant factors and establishing necessary terms and conditions to ensure the maintenance of data protection standards during international processing.

**Establishment of a Data Protection Board:** The Data Protection Board will function as an impartial adjudicatory body responsible for resolving privacy-related grievances and disputes between relevant parties. As an independent regulator, it will possess the authority to ascertain instances of non-compliance with the Act's provisions and impose penalties accordingly. The appointment of the chief executive and board members of the Data Protection Board will be carried out by the central government, ensuring a fair and transparent selection process. To provide an avenue for customers to challenge decisions made by the Data Protection Board, the government will establish an appellate body. This appellate body may be assigned to the Telecom Disputes Settlement and Appellate Tribunal (TDSAT), which will be responsible for adjudicating disputes related to data protection and hearing appeals against the decisions made by the Data Protection Board.

**Voluntary undertaking:** Under this provision, the Data Protection Board has the authority to accept a voluntary commitment related to compliance with the DPDP Act's provisions from any data fiduciary at any stage of complaint proceedings. This voluntary undertaking may entail specific actions to be taken or refrained from by the concerned party. Furthermore, the terms of the voluntary undertaking can be modified by the Board if necessary. The voluntary undertaking serves as a legal barrier to proceedings concerning the subject matter of the commitment, unless the data fiduciary fails to adhere to its terms. In the event of non-compliance, such a breach is considered a violation of the DPDP Act, and the Board is authorized to impose penalties for this infringement. Additionally, the Board has the discretion to require the undertaking to be made public.

**Alternate disclosure mechanism:** This mechanism will allow two parties to settle their complaints with the help of a mediator.

**Offence and penalties:** Data fiduciaries can face penalties of up to INR 2.5 billion for failing to comply with the provisions. These include: penalties of up to INR 10,000 for breach of the duty towards data principals; penalty up to INR 2.5 billion for failing to take reasonable security safeguards to prevent breach of personal data; fines up to INR 2 billion for failure to notify the Data Protection Board and affected data principals in case of a personal data breach; penalties of up to INR 2 billion for violation of additional obligations related to children's data; penalty of INR 1.5 billion for failure to comply with additional obligations of significant data fiduciary; penalty of INR 500 million for breach of any other provision of the DPDP Act, 2023 and rules made thereunder.

**Conflict with existing laws:** The provisions of the DPDP Act will be in addition to and not supersede any

other law currently in effect. However, in case of any conflict between a provision of this Act and a provision of any other law currently in effect, the provision of this Act shall take precedence to the extent of such conflict.

### **Exemptions under the DPDP Act**

The exemptions provided in the DPDP Act are as follows:

- For notified agencies, in the interest of security, sovereignty, public order, etc.
- For research, archiving, or statistical purposes.
- For start-ups or other notified categories of data fiduciaries.
- To enforce legal rights and claims.
- To perform judicial or regulatory functions.
- To prevent, detect, investigate, or prosecute offences.
- To process in India personal data of non-residents under foreign contract.
- For approved merger, demerger, etc.
- To locate defaulters and their financial assets etc.

### **Steps for companies prepare for compliance under the Digital Personal Data Protection Act**

By following the below steps, companies can prepare for compliance with India's DPDP Act and protect personal data in line with regulatory guidelines.

#### *Assess and build data privacy:*

- Evaluate current compliance status.
- Create a phased action plan covering governance, technology, people, and processes.
- Establish a privacy organization with defined roles, including the DPO, especially if your entity's status is an SDF.

#### *Inventory personal data systems:*

- Identify critical data storage and processing systems.

#### *Identify data processors:*

- List third parties handling personal data.
- Update agreements and communicate responsibilities.

#### *Draft DPDP Act-compliant documents:*

- Create approved data privacy policies and processes.
- Update necessary documents.
- Develop privacy notices, consent forms, and standard contract clauses.

#### *Design consent mechanisms:*

- Define consent types.
- Develop user-friendly consent processes.
- Implement efficient consent management tools.

*Establish data principal rights handling:*

- Set up processes for addressing data principal rights.
- Develop procedures for request handling.
- Use tools for efficient rights management.

*Implement data breach response:*

- Create breach management processes.
- Integrate with incident management.

*Define data retention periods:*

- Categorize data and align retention periods with requirements.

*Evaluate and implement privacy technologies:*

- Choose suitable tech solutions.
- Assess compatibility and scalability.
- Implement chosen solutions.

*Conduct communication and awareness programs:*

- Develop plans and materials.
- Launch awareness initiatives.
- Provide training to stakeholders.

*Monitor government notifications:*

- Stay updated on Central Government notifications and any forthcoming rules under the Act.
- Take necessary actions based on government directives.

## **European Union Artificial Intelligence Act, 2024 (AI Act)<sup>29</sup>**

The Artificial Intelligence Act (AI Act) is European Union regulation on artificial intelligence (AI) in the European Union. It aims to establish a common regulatory and legal framework for AI. Proposed by the European Commission on 21 April 2021 and passed in the European Parliament on 13 March 2024, it awaits reading in the EU Council.

Its scope would encompass all types of AI in a broad range of sectors (exceptions include AI systems used solely for military, national security, research, and non-professional purpose). As a piece of product

---

<sup>29</sup> Reproduced from *Artificial Intelligence Act*. Available at [https://commission.europa.eu/news/ai-act-enters-force-2024-08-01\\_en](https://commission.europa.eu/news/ai-act-enters-force-2024-08-01_en)

regulation, it would not confer rights on individuals, but would regulate the providers of AI systems, and entities using AI in a professional context.

The AI Act was revised following the rise in popularity of generative AI systems such as ChatGPT, whose general-purpose capabilities present different stakes and did not fit the defined framework. More restrictive regulations are planned for powerful generative AI systems with systemic impact.

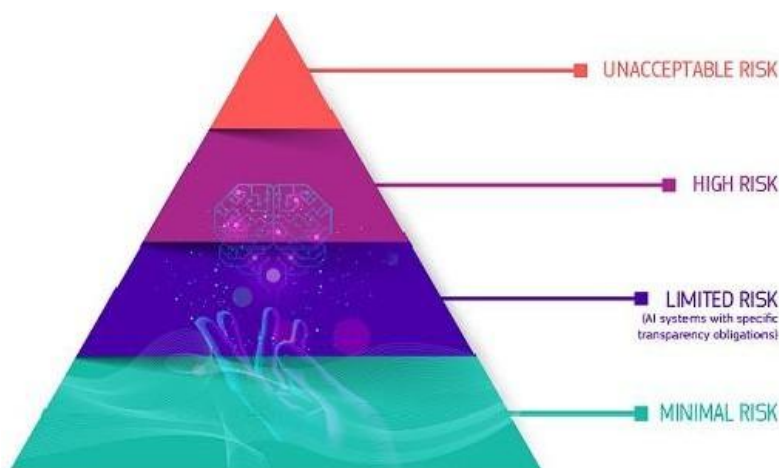
### Summary of European Union AI Act

The European Union Artificial Intelligence Act is finally herewith extra-territorial reach and wide-reaching ramifications for providers, deployers, and users of Artificial Intelligence (“AI”), the Artificial Intelligence Act (“AI Act”) was finally approved by the European Parliament (“EP”) on March 13, 2024. The text of the approved version is based on the political agreement that the EP reached with the Council of the European Union in December 2023. Members of the EP passed the law with 523 votes in favor, 46 against, and 49 abstentions. The Act aims to safeguard the use of AI systems within the EU as well as prohibiting certain AI outright.

The AI Act applies to:

- providers placing AI systems or models on the market in the EU or putting into service AI systems or placing on the market general-purpose AI models in the EU, irrespective of whether those providers are located within or outside the EU;
- deployers of AI systems that have their place of establishment in or who are located within the EU;
- providers and deployers of AI systems that have their place of establishment or who are located in a third country in situations where the output produced by the AI system is used in the EU;
- importers and distributors of AI systems into or within the EU;
- product manufacturers who place an AI system on the market or put it into service an AI system within the EU together with their product and under their own name or trademark;
- authorized representatives of AI systems where such providers are not established in the EU; and
- affected persons or citizens located in the EU.

### Four (4) Point Summary of European Union AI



- **Minimal Risk:** most AI systems such as spam filters and AI-enabled video games face no obligation under the AI Act, but companies can voluntarily adopt additional codes of conduct.
- **Limited Risk/Specific Transparency Risk:** systems like chatbots must clearly inform users that they are interacting with a machine, while certain AI-generated content must be labelled as such.
- **High Risk:** high-risk AI systems such as AI-based medical software or AI systems used for recruitment must comply with strict requirements, including risk-mitigation systems, high-quality of data sets, clear user information, human oversight, etc.
- **Unacceptable Risk:** for example, AI systems that allow “social scoring” by governments or companies are considered a clear threat to people's fundamental rights and are therefore banned.

**The majority of obligations fall on providers (developers) of high-risk AI systems.**

- Those that intend to place on the market or put into service high-risk AI systems in the EU, regardless of whether they are based in the EU or a third country.
- And also third country providers where the high risk AI system’s output is used in the EU.

**Users are natural or legal persons that deploy an AI system in a professional capacity, not affected end-users.**

- Users (deployers) of high-risk AI systems have some obligations, though less than providers (developers).
- This applies to users located in the EU, and third country users where the AI system’s output is used in the EU.

**General Purpose AI (GPAI):**

- All GPAI model providers must provide technical documentation, instructions for use, comply with the Copyright Directive, and publish a summary about the content used for training.
- All providers of GPAI models that present a systemic risk – open or closed – must also conduct model evaluations, adversarial testing, track and report serious incidents and ensure cybersecurity protections.

**AI Systems:**

- deploying subliminal, manipulative, or deceptive techniques to distort behaviour and impair informed decision-making, causing significant harm.
- exploiting vulnerabilities related to age, disability, or socio-economic circumstances to distort behaviour, causing significant harm.
- biometric categorisation systems inferring sensitive attributes (race, political opinions, trade union membership, religious or philosophical beliefs, sex life, or sexual orientation), except labelling or filtering of lawfully acquired biometric datasets or when law enforcement categorises biometric data.
- social scoring, i.e., evaluating or classifying individuals or groups based on social behaviour or personal traits, causing detrimental or unfavourable treatment of those people.
- assessing the risk of an individual committing criminal offenses solely based on profiling or personality traits, except when used to augment human assessments based on objective, verifiable facts directly linked to criminal activity.
- compiling facial recognition databases by untargeted scraping of facial images from the internet or CCTV footage.
- inferring emotions in workplaces or educational institutions, except for medical or safety reasons.

- ‘real-time’ remote biometric identification (RBI) in publicly accessible spaces for law enforcement, except when:
- searching for missing persons, abduction victims, and people who have been human trafficked or sexually exploited;
- preventing substantial and imminent threat to life, or foreseeable terrorist attack; or
- identifying suspects in serious crimes (e.g., murder, rape, armed robbery, narcotic and illegal weapons trafficking, organised crime, and environmental crime, etc.).
- Free and open licence GPAI model providers only need to comply with copyright and publish the training data summary, unless they present a systemic risk.

Once an AI system is on the market, authorities are in charge of market surveillance, deployers ensure human oversight and monitoring, and providers have a post-market monitoring system in place. Providers and deployers will also report serious incidents and malfunctioning.

## **Governance**

### **How will the AI Act be implemented?**

- The AI Office will be established, sitting within the Commission, to monitor the effective implementation and compliance of GPAI model providers.
- Downstream providers can lodge a complaint regarding the upstream providers infringement to the AI Office.

The AI Office may conduct evaluations of the GPAI model to:

- assess compliance where the information gathered under its powers to request information is insufficient.
- Investigate systemic risks, particularly following a qualified report from the scientific panel of independent experts.

## **Timelines**

After entry into force, the AI Act will apply:

- 6 months for prohibited AI systems.
- 12 months for GPAI.
- 24 months for high risk AI systems under Annex III.
- 36 months for high risk AI systems under Annex II.

## **Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021<sup>30</sup>**

In year 2021, Government notified Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021

Amidst growing concerns around lack of transparency, accountability and rights of users related to digital media and after elaborate consultation with the public and stakeholders, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 has been framed in exercise of powers

<sup>30</sup> Reproduced from Press Information Bureau of India. Available at <https://pib.gov.in/Pressreleaseshare.aspx?PRID=1700749>

under section 87 (2) of the Information Technology Act, 2000 and in supersession of the earlier Information Technology (Intermediary Guidelines) Rules 2011.

While finalizing these Rules, both the Ministries of Electronics and Information Technology and Ministry of Information and Broadcasting undertook elaborate consultations among themselves in order to have a harmonious, soft-touch oversight mechanism in relation to social media platform as well as digital media and OTT platforms etc.

Part- II of these Rules shall be administered by Ministry of Electronics and IT, while Part-III relating to Code of Ethics and procedure and safeguards in relation to digital media shall be administered by the Ministry of Information and Broadcasting.

### **Background:**

The Digital India programme has now become a movement which is empowering common Indians with the power of technology. The extensive spread of mobile phones, Internet etc. has also enabled many social media platforms to expand their footprints in India. Common people are also using these platforms in a very significant way. Some portals, which publish analysis about social media platforms and which have not been disputed, have reported the following numbers as user base of major social media platforms in India:

- WhatsApp users: 53 Crore
- YouTube users: 44.8 Crore
- Facebook users: 41 Crore
- Instagram users: 21 Crore
- Twitter users: 1.75 Crore

These social platforms have enabled common Indians to show their creativity, ask questions, be informed and freely share their views, including criticism of the Government and its functionaries. The Government acknowledges and respects the right of every Indian to criticize and disagree as an essential element of democracy. India is the world's largest open Internet society and the Government welcomes social media companies to operate in India, do business and also earn profits. However, they will have to be accountable to the Constitution and laws of India.

Proliferation of social media, on one hand empowers the citizens then on the other hand gives rise to some serious concerns and consequences which have grown manifold in recent years. These concerns have been raised from time to time in various forums including in the Parliament and its committees, judicial orders and in civil society deliberations in different parts of country. Such concerns are also raised all over the world and it is becoming an international issue.

Of late, some very disturbing developments are observed on the social media platforms. Persistent spread of fake news has compelled many media platforms to create fact-check mechanisms. Rampant abuse of social media to share morphed images of women and contents related to revenge porn have often threatened the dignity of women. Misuse of social media for settling corporate rivalries in blatantly unethical manner has become a major concern for businesses. Instances of use of abusive language, defamatory and obscene contents and blatant disrespect to religious sentiments through platforms are growing.

Over the years, the increasing instances of misuse of social media by criminals, anti-national elements have brought new challenges for law enforcement agencies. These include inducement for recruitment of terrorists, circulation of obscene content, spread of disharmony, financial frauds, incitement of violence,

public order etc.

It was found that currently there is no robust complaint mechanism wherein the ordinary users of social media and OTT platforms can register their complaint and get it redressed within defined timeline. Lack of transparency and absence of robust grievance redressal mechanism have left the users totally dependent on the whims and fancies of social media platforms. Often it has been seen that a user who has spent his time, energy and money in developing a social media profile is left with no remedies in case that profile is restricted or removed by the platform without giving any opportunity to be heard.

### **Evolution of social media and Other Intermediaries:**

If we notice the evolution of social media intermediaries, they are no longer limited to playing the role of pure intermediary and often they become publishers. These Rules are a fine blend of liberal touch with gentle self-regulatory framework. It works on the existing laws and statutes of the country which are applicable to content whether online or offline. In respect of news and current affairs publishers are expected to follow the journalistic conduct of Press Council of India and the Programme Code under the Cable Television Network Act, which are already applicable to print and TV. Hence, only a level playing field has been proposed.

### **Rationale and Justification for New Guidelines:**

These Rules substantially empower the ordinary users of digital platforms to seek redressal for their grievances and command accountability in case of infringement of their rights. In this direction, the following developments are noteworthy:

- The Supreme Court in suo-moto writ petition (Prajjawala case) vide order dated 11/12/2018 had observed that the Government of India may frame necessary guidelines to eliminate child pornography, rape and gangrape imageries, videos and sites in content hosting platforms and other applications.
- The Supreme Court vide order dated 24/09/2019 had directed the Ministry of Electronics and Information Technology to apprise the timeline in respect of completing the process of notifying the new rules.
- There was a Calling Attention Motion on the misuse of social media and spread of fake news in the Rajya Sabha and the Minister had conveyed to the house on 26/07/2018, the resolve of the Government to strengthen the legal framework and make the social media platforms accountable under the law. He had conveyed this after repeated demands from the Members of the Parliament to take corrective measures.
- The Ad-hoc committee of the Rajya Sabha laid its report on 03/02/2020 after studying the alarming issue of pornography on social media and its effect on children and society as a whole and recommended for enabling identification of the first originator of such contents.

### **Consultations:**

The Ministry of Electronics and Information Technology (MeitY) prepared draft Rules and invited public comments on 24/12/2018. MeitY received 171 comments from individuals, civil society, industry association and organizations. 80 counter comments to these comments were also received. These comments were analyzed in detail and an inter-ministerial meeting was also held and accordingly, these Rules have been finalized.

## Salient Features

Guidelines Related to Social Media to Be Administered by Ministry of Electronics and IT:

- ***Due Diligence To Be Followed By Intermediaries:*** The Rules prescribe due diligence that must be followed by intermediaries, including social media intermediaries. In case, due diligence is not followed by the intermediary, safe harbour provisions will not apply to them.
- ***Grievance Redressal Mechanism:*** The Rules seek to empower the users by mandating the intermediaries, including social media intermediaries, to establish a grievance redressal mechanism for receiving resolving complaints from the users or victims. Intermediaries shall appoint a Grievance Officer to deal with such complaints and share the name and contact details of such officer. Grievance Officer shall acknowledge the complaint within twenty four hours and resolve it within fifteen days from its receipt.
- ***Ensuring Online Safety and Dignity of Users, Specially Women Users:*** Intermediaries shall remove or disable access within 24 hours of receipt of complaints of contents that exposes the private areas of individuals, show such individuals in full or partial nudity or in sexual act or is in the nature of impersonation including morphed images etc. Such a complaint can be filed either by the individual or by any other person on his/her behalf.
- ***Two Categories of Social Media Intermediaries:*** To encourage innovations and enable growth of new social media intermediaries without subjecting smaller platforms to significant compliance requirement, the Rules make a distinction between social media intermediaries and significant social media intermediaries. This distinction is based on the number of users on the social media platform. Government is empowered to notify the threshold of user base that will distinguish between social media intermediaries and significant social media intermediaries. The Rules require the significant social media intermediaries to follow certain additional due diligence.

Additional Due Diligence to be followed by Significant Social Media Intermediary:

- Appoint a Chief Compliance Officer who shall be responsible for ensuring compliance with the Act and Rules. Such a person should be a resident in India.
- Appoint a Nodal Contact Person for 24x7 coordination with law enforcement agencies. Such a person shall be a resident in India.
- Appoint a Resident Grievance Officer who shall perform the functions mentioned under Grievance Redressal Mechanism. Such a person shall be a resident in India.
- Publish a monthly compliance report mentioning the details of complaints received and action taken on the complaints as well as details of contents removed proactively by the significant social media intermediary.
- Significant social media intermediaries providing services primarily in the nature of messaging shall enable identification of the first originator of the information that is required only for the purposes of prevention, detection, investigation, prosecution or punishment of an offence related to sovereignty and integrity of India, the security of the State, friendly relations with foreign States, or public order or of incitement to an offence relating to the above or in relation with rape, sexually

explicit material or child sexual abuse material punishable with imprisonment for a term of not less than five years. Intermediary shall not be required to disclose the contents of any message or any other information to the first originator.

- Significant social media intermediary shall have a physical contact address in India published on its website or mobile app or both.
- Voluntary User Verification Mechanism: Users who wish to verify their accounts voluntarily shall be provided an appropriate mechanism to verify their accounts and provided with demonstrable and visible mark of verification.
- Giving Users An Opportunity to Be Heard: In cases where significant social media intermediaries removes or disables access to any information on their own accord, then a prior intimation for the same shall be communicated to the user who has shared that information with a notice explaining the grounds and reasons for such action. Users must be provided an adequate and reasonable opportunity to dispute the action taken by the intermediary.
- Removal of Unlawful Information: An intermediary upon receiving actual knowledge in the form of an order by a court or being notified by the Appropriate Govt. or its agencies through authorized officer should not host or publish any information which is prohibited under any law in relation to the interest of the sovereignty and integrity of India, public order, friendly relations with foreign countries etc.
- The Rules will come in effect from the date of their publication in the gazette, except for the additional due diligence for significant social media intermediaries, which shall come in effect 3 months after publication of these Rules.

### **Digital Media Ethics Code Relating to Digital Media and OTT Platforms to Be Administered by Ministry of Information and Broadcasting:**

There have been widespread concerns about issues relating to digital contents both on digital media and OTT platforms. Civil Society, film makers, political leaders including Chief Minister, trade organizations and associations have all voiced their concerns and highlighted the imperative need for an appropriate institutional mechanism. The Government also received many complaints from civil society and parents requesting interventions. There were many court proceedings in the Supreme Court and High Courts, where courts also urged the Government to take suitable measures.

Since the matter relates to digital platforms, therefore, a conscious decision was taken that issues relating to digital media and OTT and other creative programmes on Internet shall be administered by the Ministry of Information and Broadcasting but the overall architecture shall be under the Information Technology Act, which governs digital platforms.

#### **Consultations:**

Ministry of Information and Broadcasting held consultations in Delhi, Mumbai and Chennai over the last one and half years wherein OTT players have been urged to develop “self-regulatory mechanism”. The Government also studied the models in other countries including Singapore, Australia, EU and UK and has gathered that most of them either have an institutional mechanism to regulate digital content or are in the process of setting-up one.

The Rules establish a soft-touch self-regulatory architecture and a Code of Ethics and three tier grievance redressal mechanism for news publishers and OTT Platforms and digital media.

Notified under section 87 of Information Technology Act, these Rules empower the Ministry of Information and Broadcasting to implement Part-III of the Rules which prescribe the following:

- Code of Ethics for online news, OTT platforms and digital media: This Code of Ethics prescribe the guidelines to be followed by OTT platforms and online news and digital media entities.
- Self-Classification of Content: The OTT platforms, called as the publishers of online curated content in the rules, would self-classify the content into five age based categories- U (Universal), U/A 7+, U/A 13+, U/A 16+, and A (Adult). Platforms would be required to implement parental locks for content classified as U/A 13+ or higher, and reliable age verification mechanisms for content classified as “A”. The publisher of online curated content shall prominently display the classification rating specific to each content or programme together with a content descriptor informing the user about the nature of the content, and advising on viewer description (if applicable) at the beginning of every programme enabling the user to make an informed decision, prior to watching the programme.
- Publishers of news on digital media would be required to observe Norms of Journalistic Conduct of the Press Council of India and the Programme Code under the Cable Television Networks Regulation Act thereby providing a level playing field between the offline (Print, TV) and digital media.
- A three-level grievance redressal mechanism has been established under the rules with different levels of self-regulation.  
Level-I: Self-regulation by the publishers;  
Level-II: Self-regulation by the self-regulating bodies of the publishers;  
Level-III: Oversight mechanism.
- Self-regulation by the Publisher: Publisher shall appoint a Grievance Redressal Officer based in India who shall be responsible for the redressal of grievances received by it. The officer shall take decision on every grievance received by it within 15 days.
- Self-Regulatory Body: There may be one or more self-regulatory bodies of publishers. Such a body shall be headed by a retired judge of the Supreme Court, a High Court or independent eminent person and have not more than six members. Such a body will have to register with the Ministry of Information and Broadcasting. This body will oversee the adherence by the publisher to the Code of Ethics and address grievances that have not been resolved by the publisher within 15 days.
- Oversight Mechanism: Ministry of Information and Broadcasting shall formulate an oversight mechanism. It shall publish a charter for self-regulating bodies, including Codes of Practices. It shall establish an Inter-Departmental Committee for hearing grievances.

### **MeitY releases Draft Digital Personal Data Protection Rules, 2025<sup>31</sup>**

Ministry of Electronics and Information Technology has drafted the Digital Personal Data Protection Rules, 2025 to facilitate the implementation of the Digital Personal Data Protection Act, 2023 (DPDP Act). It aims to strengthen the legal framework for the protection of digital personal data by providing necessary details and an actionable framework. Stakeholder are invited to share feedback/comments on the draft Rules.

---

<sup>31</sup><https://www.meity.gov.in/static/uploads/2025/02/f8a8e97a91091543fe19139cac7514a1.pdf>

The draft Rules details about the various implementation aspects such as the notice by the Data Fiduciary to the individuals, registration and obligations of Consent Manager, processing of personal data for issuance of subsidy, benefit, service etc. by State, applicability of reasonable security safeguards, intimation of personal data breach, providing details about availing of their rights by the individuals, processing of personal data of child or of person with disability, setting up the Data Protection Board, appointment and service conditions of the Chairperson and other members of the Board, functioning of Board as digital office, procedure to appeal to Appellate Tribunal among others.

### **India Cyber Threat Report 2025<sup>32</sup>**

The cybersecurity landscape in India has witnessed an unprecedented evolution throughout 2024, marked by both escalating threats and significant advances in detection capabilities. This summary outlines the critical findings that shape India's current cybersecurity posture and its implications for the future. First, the sheer scale of cyber threats is staggering. The detection of over 369.01 million security incidents across 8.44 million endpoints means that, on average, every minute sees 702 potential security threats. To put this in perspective, this is roughly equivalent to having eleven new cyber threats emerging every second somewhere in India. This volume of attacks demonstrate the relentless nature of modern cyber threats and the constant pressure on security systems. A particularly noteworthy development is the significant shift in how malware is being detected. The increase in behavior-based detections from 12.5% to 14.5% represents an important evolution in both attack and defense strategies. This change tells us that attackers are creating more sophisticated malware that can evade traditional signature-based detection methods. The geographical distribution of attacks reveals an interesting pattern about how cyber threats are spreading across India. While major tech hubs like Telangana (15.03% of detections) and Tamil Nadu (12%) remain primary targets, we're seeing increasing activity in Tier 2 cities. This suggests that cybercriminals are expanding their reach beyond traditional targets, possibly because smaller cities might have less robust cyber defenses. The healthcare industry's position as the most attacked sector (21.82% of all attacks) is particularly concerning. This likely reflects the high value of medical data and the critical nature of healthcare systems, which might make organizations more likely to pay ransoms. The significant targeting of hospitality (19.57%) and banking sectors (17.38%) suggests that attackers are focusing on industries that handle large volumes of personal and financial data.

The rise in cloud-based detections is especially significant, with 62% of detections occurring in cloud environments. This reflects the broader digital transformation across Indian businesses, but it also highlights a critical security challenge. As more organizations move their operations to the cloud, they're creating new opportunities for attackers to exploit misconfigured or inadequately protected cloud resources. In 2025, the cyber threat landscape will be dominated by AI-driven attacks, with cybercriminals leveraging generative AI to create more sophisticated and adaptive threats using AI-powered malware. Social media and generative AI will enable highly targeted scams and impersonations, making it harder to distinguish between real and artificial interactions. Ransomware will continue to evolve, targeting supply chains and critical infrastructure. The rise of cloud adoption is likely to expose misconfigured cloud environments and insecure APIs, resulting in attackers exploiting cloud vulnerabilities. Supply chain complexities in hardware will continue to pose challenges with tampered devices and IoT infrastructure. Fake apps, especially in the fintech and government sectors, will remain a significant concern. Additionally, the challenging geopolitical situation is likely to result in state actors targeting critical infrastructure and public utility services.

<sup>32</sup>file:///C:/Users/HP/Downloads/India-Cyber-Threat-Report-2025.pdf

In addition to presenting a detailed overview of the current cyber threat landscape, this report delves into a PESTLE analysis, offering valuable insights into the macro impact of cyber threats across various dimensions. The Political aspect examines how cyber threats influence national security, government policies, and international relations. Economically, the report highlights the financial repercussions of cyber incidents, including costs related to data breaches, fraud, and business disruptions. The social dimension explores the effects on public trust, privacy concerns, and the societal implications of widespread cyber attacks. Legally, the analysis addresses the evolving regulatory landscape and the importance of compliance with cybersecurity laws and standards. Technologically, the report underscores the advancements in cyber defense mechanisms and the continuous innovation required to counteract sophisticated threats. Lastly, the environmental aspect considers the indirect impact of cyber threats on critical infrastructure and the potential consequences for environmental sustainability. This comprehensive PESTLE analysis aims to provide a holistic understanding of the far-reaching implications of cyber threats, guiding stakeholders in developing robust strategies to mitigate risks and enhance resilience. The trends reported suggest that organizations need to take a more comprehensive approach to cybersecurity. This means not just investing in technical solutions, but also in training employees, developing incident response plans, and building relationships with security partners. The rise in politically motivated cyber attacks also indicates that organizations need to consider geopolitical factors in their security planning. These findings paint a picture of a rapidly evolving threat landscape where traditional security approaches alone are no longer sufficient. Organizations need to adapt their security strategies to address both current and emerging threats while maintaining vigilance against traditional attack vectors. The report makes it clear that cybersecurity is no longer just an IT issue but a fundamental business risk that requires attention at all levels of an organization.

## Lesson 4- Cyber Crimes and Investigation Procedures

### **India is the 80th most targeted country worldwide in cybercrime: Report<sup>33</sup>**

It is stated in an article of The Hindu, with the rise of AI use and the consistent digital payment adoption here, it has become imperative for organizations to continuously improve their cybersecurity posture to protect their assets and maintain stakeholder trust.

As per the Report published on recording the cyber incidents, India was placed on the 80th position in a report focusing on local threats in the year 2023. The position is based on the malicious programs found directly on users' computers or removable media connected to them (flash drives, camera memory cards, phones, external hard drives) or that initially made their way onto the computer in non-open form, including programs in complex installers or encrypted files.

Additionally, nearly 34% of users in India were targeted by local threats, amounting to some 74,385,324 local incidents being blocked by one of the leading antivirus companies.

India's cybersecurity market reached USD 6.06 billion in 2023. However, according to IDC, a global marketing intelligence firm, the alarming increase in sophisticated external cyber threats and cybersecurity attacks is one of the biggest challenges for the majority of enterprises in establishing organizational trust.

Almost 67% of Indian enterprises are reportedly looking to outsource key areas of security landscape to managed security service providers in the next three years.

### **Central Government Initiative on Strengthening Mechanism to Lever Cyber Crimes<sup>34</sup>**

The Central Government supplements the initiatives of the States/UTs through advisories and financial assistance under various schemes for capacity building of their Law Enforcement Agencies (LEAs). To strengthen the mechanism to deal with cyber-crimes in a comprehensive and coordinated manner, the Central Government has taken steps which, inter-alia, include the following:

- The Ministry of Home Affairs has set up the 'Indian Cyber Crime Coordination Centre' (I4C) to deal with all types of cyber-crime in the country, in a coordinated and comprehensive manner.
- Seven Joint Cyber Coordination Teams (JCCTs) have been constituted for Mewat, Jamtara, Ahmedabad, Hyderabad, Chandigarh, Vishakhapatnam, and Guwahati under I4C covering the whole country based upon cyber-crime hotspots/ areas having multi-jurisdictional issues by on boarding States/UTs to enhance the coordination framework among the Law Enforcement Agencies of the States/UTs. Seven workshops were organized for JCCTs at Hyderabad, Ahmedabad, Guwahati, Vishakhapatnam, Lucknow, Ranchi and Chandigarh in 2023.

---

<sup>33</sup>Reproduced from The Hindu. Available at <https://www.thehindu.com/sci-tech/technology/india-the-80-most-targeted-country-worldwide-in-cybercrime/article67869960.ece>

<sup>34</sup> Reproduced from Increase in Cyber Crime (February 07, 2024), Information was given by Minister of State for Home Minister in a written reply to Rajya Sabha, Press Information Bureau. Available at <https://pib.gov.in/PressReleaseIframePage.aspx?PRID=2003505>

- National Cyber Forensic Laboratory (Investigation) has been established, as a part of the I4C, at New Delhi to provide early stage cyber forensic assistance to Investigating Officers (IOs) of State/UT Police. So far, National Cyber Forensics Laboratory (Investigation) have provided its services to State LEAs in around 9,000 cyber forensics like mobile forensics, memory forensics, Call Data Record (CDR) Analysis, etc. to help them in investigation of cases pertaining to cyber-crimes.
- The ‘National Cyber Crime Reporting Portal’ (<https://cybercrime.gov.in>) has been launched, as a part of the I4C, to enable public to report incidents pertaining to all types of cyber-crimes, with special focus on cybercrimes against women and children. Cyber-crime incidents reported on this portal, their conversion into FIRs and subsequent action thereon are handled by the State/UT Law Enforcement Agencies concerned as per the provisions of the law.
- The ‘Citizen Financial Cyber Fraud Reporting and Management System’, under I4C, has been launched for immediate reporting of financial frauds and to stop siphoning off funds by the fraudsters. So far, an amount of more than Rs. 1200 Crore have been saved in more than 4.7 lakh complaints. A toll-free Helpline number ‘1930’ has been operationalized to get assistance in lodging online cyber complaints.
- The Massive Open Online Courses (MOOC) platform, namely ‘CyTrain’ portal has been developed under I4C, for capacity building of police officers/judicial officers through online course on critical aspects of cyber-crime investigation, forensics, prosecution etc. along with certification. More than 76,000 Police Officers from States/UTs are registered and more than 53,000 Certificates issued through the portal.
- Till date more than 3.2 lakhs SIM cards and 49,000 IMEIs as reported by Police authorities have been blocked by Government of India.
- I4C has imparted cyber hygiene training to 6,000 officials of various Ministries/ Departments of Government of India.
- I4C has imparted cyber hygiene training to more than 23,000 NCC cadets.
- The Ministry of Home Affairs has provided financial assistance to the tune of Rs. 122.24 crores under the ‘Cyber Crime Prevention against Women and Children (CCPWC)’ Scheme, to the States/UTs for their capacity building such as setting up of cyber forensic-cum-training laboratories, hiring of junior cyber consultants and training of LEAs’ personnel, public prosecutors and judicial officers. So far, cyber forensic-cum-training laboratories have been commissioned in 33 States/UTs. So far, more than 24,600 LEA personnel, judicial officers and prosecutors have been provided training on cyber-crime awareness, investigation, forensics etc.
- National Cyber Forensic Laboratory (Evidence) has been set up at Hyderabad. Establishment of this laboratory provides the necessary forensic support in cases of evidence related to cyber-crime, preserving the evidence and its analysis in line with the provisions of IT Act and Evidence Act; and reduced turnaround time.
- To spread awareness on cyber-crime, the Central Government has taken steps which, inter-alia, include; dissemination of messages through SMS, I4C social media account i.e. X (formerly Twitter) (@Cyberdost), Facebook (CyberDostI4C), Instagram (cyberdosti4C), Telegram (cyberdosti4c), Radio campaign, engaged MyGov for publicity in multiple mediums, organizing Cyber Safety and Security Awareness weeks in association with States/UTs, publishing of Handbook for Adolescents/Students, etc. The States/UTs have also been requested to carry out publicity to create mass awareness.

- CERT-In issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers, mobile phones, networks and data on an ongoing basis.
- CERT-In, through RBI, has advised all authorized entities and banks issuing pre-paid payment instruments (wallets) in the country to carry out special audit by CERT-In-empaneled auditors, close the non-compliances identified in the audit report and ensure implementation of security best practices.
- CERT-In and the Reserve Bank of India (RBI) jointly carry out a cyber security awareness campaign on 'beware and be aware of financial frauds' through the Digital India Platform.

### **Some of the common cyber-crimes of 2023-2024<sup>35</sup>**

- **FedEx Scam**

How it works: It all starts when someone gets a call from a stranger pretending to be from 'FedEx.' The caller says a package in the person's name, heading to Macau or another country, got seized by Mumbai customs for having illegal stuff. After that, the victim is linked to a "police officer," often from the Mumbai Crime Branch or Anti-Narcotics Unit.

Protect yourself: Verify the legitimacy of such messages/calls by contacting FedEx directly using official contact information.

- **YouTube Like Scam**

How it works: Criminals are using WhatsApp and Telegram to approach potential victims with offers for part-time work from home or part-time jobs. In these fraudulent schemes, scammers are enticing users to engage with videos on YouTube by liking and subscribing.

Protect yourself: Avoid clicking on links in suspicious messages. Verify notifications directly on the official YouTube website or app.

- **Online Shopping Scam**

How it works: Fraudsters make fake websites that seem like real online stores. These sites usually tempt people with attractive discounts on popular products to trick them. When people enter their payment details, the scammers take their money and vanish.

Protect yourself: Stick to well-known online stores, check reviews, and be wary of deals that appear too good to be true. Opt for secure payment options, and ensure the website has a secure connection before making any purchases.

- **Identity Theft Scam**

How it works: Identity theft occurs when someone dishonestly obtains another person's important personal and financial information. They then use this information for various fraudulent activities, posing a

---

<sup>35</sup> Reproduced from Cyber Digest (2024), Indian Cyber Crime Coordination, Ministry of Home Affairs. Available at [https://i4c.mha.gov.in/cyber\\_digest/jan\\_2024/I4C%20Daily%20Digest-%2029.01.2024%20.pdf](https://i4c.mha.gov.in/cyber_digest/jan_2024/I4C%20Daily%20Digest-%2029.01.2024%20.pdf)

significant risk to the victim.

Protect yourself: Create strong and unique passwords, turn on two-factor authentication, be careful about sharing personal details on the internet, and routinely keep an eye on your accounts for any unusual activities.

- **Scholarship and Grant Scam**

How it works: Be wary of scammers pretending to be organizations offering scholarships or grants. They might ask for upfront fees or personal information without any intention of actually providing financial assistance.

Protect yourself: When searching for scholarships, make sure to thoroughly research your options, confirm the legitimacy of organizations, and be cautious if asked for payment or sensitive information. Legitimate scholarships usually don't involve upfront fees.

### **Cyber Security Audit: A Snapshot<sup>36</sup>**

A cybersecurity audit involves a comprehensive analysis and review of your IT infrastructure. It detects vulnerabilities and threats, displaying weak links and high-risk practices.

Significant benefits of IT security audits are:

- Risk assessment and vulnerability identification
- Strengthened security measures
- Compliance with regulations and standards
- Incident response preparedness
- Safeguarding sensitive data and customer trust
- Proactive threat detection and prevention

Cybersecurity audits ensure a 360-degree in-depth audit of your organization's security posture. They aim to identify vulnerabilities, risks, and threats that may affect the organization. These audits cover various areas, including:

- Data Security – involves reviewing network access control, encryption use, data security at rest, and transmissions.
- Operational Security – involves a review of security policies, procedures, and controls.
- Network Security – a review of network & security controls, anti-virus configurations, security monitoring capabilities, etc.

---

<sup>36</sup> Reproduced from Chinnaswamy Vinugayathri (2023), What Is Cyber Security Audit and How Is It Helpful for Your Business? Indusface. Available at <https://www.indusface.com/blog/what-is-cyber-security-audit-and-how-it-is-helpful-for-your-business/#:~:text=A%20cybersecurity%20audit%20involves%20a,Risk%20assessment%20and%20vulnerability%20identification>

- System Security – This review covers hardening processes, patching processes, privileged account management, role-based access, etc.
- Physical Security – a review that covers disk encryption, role-based access controls, biometric data, multifactor authentication, etc.

Beyond these, a cybersecurity audit can also cover cybersecurity risk management, cyber risk governance, training & awareness, legal, regulatory & contractual requirements, technical security controls, business continuity & incident management, and third-party management.

**Cyber Security Audit Checklist**

Company : \_\_\_\_\_ Date : \_\_\_\_\_

**Physical Security**

- Ensure all facilities have controlled access with appropriate authorization
- Implement video surveillance and intrusion detection systems
- Secure server rooms, network equipment, and backup storage locations
- Conduct regular security reviews of physical access controls

**Network Security**

- Update and patch all network devices, including routers, switches, and firewalls
- Implement strong authentication and encryption protocols for wireless networks
- Regularly monitor network traffic for unusual or suspicious activity
- Perform penetration tests and vulnerability assessments on a routine basis

**Data Security**

- Classify and encrypt sensitive data
- Implement strong access controls and user authentication
- Regularly back up critical data and store backups in a secure offsite location
- Implement data loss prevention (DLP) solutions and monitor for potential breaches

**Employee Training and Awareness**

- Provide ongoing cyber security awareness training for all employees
- Implement a strong password policy and require employees to use multi-factor authentication
- Educate employees on recognizing and reporting phishing and social engineering attacks
- Conduct regular security drills to test employee preparedness

**Incident Response and Recovery**

- Develop a comprehensive incident response plan
- Regularly test and update the plan to ensure its effectiveness
- Establish a dedicated incident response team with clearly defined roles and responsibilities
- Implement a disaster recovery plan and regularly test its effectiveness

**Compliance and Legal Requirements**

- Stay up-to-date with relevant industry regulations and standards
- Conduct regular audits to ensure compliance with these requirements
- Implement a risk management program to continuously assess and mitigate risks
- Consult with legal counsel to ensure your organization meets all legal obligations

Source: <https://blueteamresources.in/cyber-security-audit-checklist/>

## **Email Policy of Government of India, 2024<sup>37</sup>**

The Ministry of Electronics and Information Technology (MeitY) recently issued the “Email Policy of Government of India, 2024.” It is an updated email policy for central government employees, requiring the exclusive use of official government emails managed by the National Informatics Centre (NIC) for public duties. The policy replaces 2015 guidelines and prohibits government employees, contractors, and consultants from using their official email addresses on social media or other websites unless authorised for official functions. The policy aims to reinforce cybersecurity measures and protocols, maintain secure communications, and ensure compliance across departments. It is not legally binding, but its gazette notification ensures compliance and maintains cyber resilience in communications. The updated policy is also aligned with the newly enacted Digital Personal Data Protection Act, 2023.

### **Brief Highlights of Email Policy of Government of India, 2024**

- The Email Policy of the Government of India, 2024 is divided into three parts namely, Part I: Introduction, Part II: Terms of Use, Part III: Functions, duties and Responsibilities, and with an annexe attached to it defining the meaning of certain organisation types in relation to this policy.
- The policy direct to not use NICeMail address for registering on any social media or other websites or mobile applications, save for the performance of official duties or with due authorisation from the authority competent.
- Under this new policy, “core use organisations” (central government departments and other government-controlled entities that do not provide goods or services on commercial terms) and its users shall use only NICeMail for official purposes.
- However, where the Core Use Organisation has an office or establishment outside India, to ensure availability of local communication channels under exigent circumstances may use alternative email services hosted outside India with all due approval.
- Core Use Organisations, including those dealing with national security, have their own independent email servers and can continue operating their independent email servers provided the servers are hosted in India. They should also consider migrating their email services to NICeMail Services for security and uniform policy enforcement.
- The policy also requires departments that currently use @gov.in or @nic.in to instead migrate to @departmentname.gov.in mail domains so that information sanctity and integrity can be maintained when officials are transferred from one department/ministry to another, and so that the ministry/department doesn’t lose access to the official communication. For this, the department or ministry in question must register the domain name with NIC. For instance, MeitY has registered the mail domain @meity.gov.in. The policy gives government departments six months time period complete this migration.
- The policy also makes distinction between (1) Organisation-linked email addresses and (2) Service-linked email addresses. The policy in respect of “organisation-linked email addresses” is laid down in paragraphs 5.3.2(a) and 5.4 to 5.6.3. And the policy in respect of “service-linked email addresses” is laid down in paragraphs 5.3.2(b) and 5.7 to 5.7.2 under the official document of said policy.
- Further, the new policy includes specific directives on separating the email addresses of regular government employees from those of contractors or consultants to improve operational clarity.

---

<sup>37</sup><https://www.meity.gov.in/static/uploads/2025/02/f8a8e97a91091543fe19139cac7514a1.pdf>

## Lesson 5- Regulatory Framework on AI, Cyber Security and Cyberspace

### **Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices dated November 7, 2023<sup>38</sup>**

The RBI came out with Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices on November 7, 2023 with an objective to tighten the governance framework for technology within banking segment. Earlier, the RBI had released the Master Direction on Outsourcing of IT Services released on June 23, 2022 to strengthen control framework for better management of outsourcing of technology services.

Who all will be impacted with these Regulations:

- Banks;
- Small Financial Banks and CICs
- NBFCs
- Service Provider, Fintech and Technology Enabler

The master direction will apply to all RBI regulated entities except local area banks and NBFC-core investment companies. It prescribes procedures and framework for strategic alignment, risk management, resource management, performance management and business continuity/ disaster recovery management. It also provides for periodic reviews of risks, IT and information security risk management framework, information security policy and cyber security policy.

The framework provides for the constitution of three major committees by the regulated entities — IT strategy committee of the board, IT steering committee and information security committee. The regulated entities are also required to designate a senior level executive having no direct reporting relationship with the head of IT Function as ‘chief information security officer’. Further, the regulated entities have been recommended to conduct disaster recovery drills at least on a half-yearly basis for critical information and back up data in a secured manner as a business continuity measure.

These guidelines integrate consolidated and updated earlier instructions on IT Governance, Risk, Controls, Assurance Practices, and Business Continuity/Disaster Recovery Management separately released for Banks and NBFCs. Newly released Master Direction shall come into effect from April 1, 2024.

These guidelines are applicable to the following Regulated Entities (REs), unless explicitly exempted:

- Scheduled Commercial Banks (excluding Regional Rural Banks)
- Small Finance Banks
- Payments Banks
- All Non-Banking Financial Companies (NBFCs) in Top, Upper, and Middle Layers as per Scale-Based Regulation (SBR)
- All India Financial Institutions (NHB, NABARD, EXIM Bank SIDBI, and NaBFID)
- Credit Information Companies

---

<sup>38</sup> Reproduced from Charting the Course: Decoding RBI's Master Direction on IT Governance, Risk, Controls & Assurance Practices. The Digital Fifth. Available at <https://thedigitalfifth.com/decoding-rbis-master-direction-on-it-governance/>

Companies excluded from the scope are:

- Local Area Banks
- NBFC – Core Investment Companies

Regulated Entities are required to establish a robust IT Governance Framework, including governance structure and processes essential to achieve the entity's business/strategic objectives. This framework should define the roles (including authority) and responsibilities of the Board of Directors (Board), Board level Committee, Local Management Committee (in the case of foreign banks operating as branches in India), and Senior Management. It must encompass adequate oversight mechanisms to ensure accountability and mitigate business risks.

### **RBI's Updated Master Direction: Navigating the Digital Landscape Safely**

In response to the dynamic shifts in the financial sector, the Reserve Bank of India (RBI) has recently launched an updated Master Direction, reflecting the profound changes brought about by digital technologies. This article delves into the key drivers behind this strategic move and explores the thematic objectives set by the RBI to strengthen IT governance, risk management, and resilience in the banking sector.

- **Technology becoming central to Banking & Lending services:** Banks rely heavily on technology for daily operations, utilizing core banking systems, online platforms, and mobile applications. This technological dependence extends to risk management and automated decision-making, enhancing overall operational efficiency.
- **Shift in Operating Models of Banks:** The last decade has witnessed a monumental transformation in the financial sector, propelled by the advent of digital technologies. The surge in online services, coupled with competitive pressures and the need for operational efficiency, has paved the way for innovations in Mobility, AML, APIs, and Cloud Computing. These technological integrations aim to enhance service delivery, elevate customer engagement, and fortify risk management strategies.
- **Rise of Banks-FinTech's Partnership:** Collaborations between traditional financial institutions and FinTech firms have become increasingly prevalent, ushering in a new era of opportunities and challenges. While these partnerships offer benefits, they also introduce complexities in managing IT systems, encompassing aspects such as data security, system integrations, interdependencies, regulatory compliance, vendor management, and shared responsibilities.
- **Increasing impetus on Digital Transformation:** The digital transformation wave underscores the importance of agile technologies, scalability, adaptability, and resilience across the financial spectrum. The ability to navigate these facets effectively is crucial for staying competitive and meeting evolving customer expectations.
- **Continued Cyber Threats:** With increased reliance on digital technologies comes an expanded attack surface for cyber threats. This has led to a surge in cybercrimes, including DDoS attacks, phishing attempts, data breaches, and ransomware attacks. Safeguarding against these threats is imperative for maintaining the integrity of financial systems.
- **Regulatory Monitoring:** The introduction of stringent regulations, such as the Digital Personal Data Protection Act, has heightened the need for financial institutions to ensure the security and compliance of their IT systems. This regulatory scrutiny has prompted the RBI to release updated guidelines, reinforcing the importance of robust IT governance and risk management.

## **Thematic Objectives of the New RBI Master Directions:**

- Elevating the Role of the Board and Top Management: The RBI emphasizes the establishment of a Board-level IT strategy committee and an IT steering committee, underscoring the pivotal role of top management in mitigating IT risks.
- Improving Delivery Capabilities and Excellence: Encouraging best practices in software development, project management, and IT service management to enhance speed, efficiency, and quality in IT service delivery.
- Sustaining the Technology Landscape: Prioritizing regular technology updates, ongoing maintenance, and robust disaster recovery plans to ensure operational efficiency, system security, and business resilience.
- Fortifying Risk Management: Mandating regular IT risk reviews and comprehensive risk management frameworks, addressing infrastructure, security, cyber threats, and third party risks.
- Boosting Security and Resilience: Enforcing strict security controls, data encryption, regular cyber drills, and enhanced disaster recovery arrangements to fortify the overall security and resilience of IT systems.
- Enhancing Monitoring & Supervision: Calling for continuous auditing, regular vulnerability assessments, enhanced reporting on critical systems, and meticulous vendor risk management to bolster monitoring and supervision.
- 

## **SEBI Cyber Security Guidelines, 2023 – Cyber Security and Cyber Resilience framework for Portfolio Managers<sup>39</sup>**

Cyber-attacks and threats attempt to compromise the Confidentiality, Integrity, and Availability (CIA) of the computer systems, networks, and databases (Confidentiality refers to limiting access of systems and information to authorized users, Integrity is the assurance that the information is reliable and accurate, and Availability refers to guarantee of reliable access to the systems and information by authorized users). The cyber security framework includes measures, tools, and processes that are intended to prevent cyber-attacks and improve cyber resilience. Cyber Resilience is an organization's ability to prepare and respond to a cyber-attack and to continue operations during, and recover from, a cyber-attack.

With rapid technological advancement in the securities market, there is a greater need for maintaining robust cyber security and to have a cyber resilience framework to protect the integrity of data and guard against breaches of privacy.

As part of the operational risk management, the Portfolio Managers need to have robust cyber security and cyber resilience framework in order to provide essential facilities and services and perform critical functions in the securities market as Portfolio Manager.

---

<sup>39</sup> Reproduced from SEBI Circular on Cyber Security and Cyber Resilience framework for Portfolio Managers, March 29, 2023. Available at [https://www.sebi.gov.in/legal/circulars/mar-2023/cyber-security-and-cyber-resilience-framework-for-portfolio-managers\\_69521.html](https://www.sebi.gov.in/legal/circulars/mar-2023/cyber-security-and-cyber-resilience-framework-for-portfolio-managers_69521.html)

Based on feedback received from stakeholders, it has been decided that the guidelines annexed with this circular shall be effective from October 01, 2023.

In this context, Association of Portfolio Managers in India (APMI) shall also furnish activity wise implementation timelines and progress in implementation of provisions of this circular to SEBI on bi-monthly basis.

Portfolio Managers and APMI shall take necessary steps for implementing the circular, including putting the required processes and systems in place to ensure compliance with the provisions of this circular.

### **Governance**

- As part of the operational risk management framework to manage risk to systems, networks, and databases from cyber-attacks and threats, Portfolio Managers should formulate comprehensive cyber security and cyber resilience policy document encompassing the framework mentioned hereunder. The policy document should be approved by the Board or equivalent body of the Portfolio Manager, and in case of deviations from the suggested framework, reasons for such deviations should also be provided in the policy document.
- The policy document should be reviewed by the Board or equivalent body of the Portfolio Manager at least once annually with the view to strengthen and improve its cyber security and cyber resilience framework.
- The cyber security and cyber resilience policy should include the following process to identify, assess, and manage cyber security risks associated with processes, information, networks, and systems;
  - a. 'Identify' critical IT assets and risks associated with such assets,
  - b. 'Protect' assets by deploying suitable controls, tools, and measures,
  - c. 'Detect' incidents, anomalies, and attacks through appropriate monitoring tools/processes,
  - d. 'Respond' by taking immediate steps after identification of the incident, anomaly, or attack,
  - e. 'Recover' from incident through incident management, disaster recovery, and business continuity framework.
- The Cyber security policy should encompass the principles prescribed by the National Critical Information Infrastructure Protection Centre (NCIIPC) of the National Technical Research Organization (NTRO), Government of India, in the report titled 'Guidelines for Protection of National Critical Information Infrastructure' and subsequent revisions, if any, from time to time.
- Portfolio Managers should also incorporate best practices from standards such as ISO 27001, ISO 27002, COBIT 5, etc., or their subsequent revisions, if any, from time to time.
- Portfolio Managers should designate a senior official as Chief Information Security Officer (CISO) whose function would be to assess, identify and reduce cyber security risks, respond to incidents, establish appropriate standards and controls, and direct the establishment and implementation of processes and procedures as per the cyber security and resilience policy approved by the Board or equivalent body of Portfolio Manager.
- The Board or equivalent body of the Portfolio Manager shall constitute a Technology Committee comprising experts proficient in technology. This Technology Committee should on a half yearly basis review the implementation of the cyber security and cyber resilience policy approved by their

Board or equivalent body, and such review should include a review of their current IT and cyber security and cyber resilience capabilities, set goals for a target level of cyber resilience, and establish a plan to improve and strengthen cyber security and cyber resilience. The review shall be placed before the Board or equivalent body of the Portfolio Manager for appropriate action.

- The Portfolio Managers should establish a reporting procedure to facilitate communication of unusual activities and events to CISO or to the senior management in a timely manner.
- The aforementioned committee and the senior management of the Portfolio Manager, including the CISO, should periodically review instances of cyberattacks, if any, domestically and globally, and take steps to strengthen cyber security and cyber resilience framework.
- Portfolio Managers should define the responsibilities of its employees, outsourced staff, and employees of vendors and other entities, who may have access to or use systems/networks of the Portfolio Managers, towards ensuring the goal of cyber security.

### **Identify**

- Portfolio Manager shall identify and classify critical assets based on their sensitivity and criticality for business operations, services, and data management. The critical assets shall include business-critical systems, internet-facing applications/ systems, systems that contain sensitive data, sensitive personal data, sensitive financial data, Personally Identifiable Information (PII) data, etc. All the ancillary systems used for accessing/ communicating with critical systems either for operations or maintenance shall also be classified as critical assets. The Board or equivalent body of the Portfolio Manager shall approve the list of critical assets.
- To this end, Portfolio Manager shall maintain an up-to-date inventory of its hardware and systems, software and information assets (internal and external), details of its network resources, connections to its network and data flows.
- Portfolio Managers should accordingly identify cyber risks (threats and vulnerabilities) that it may face, along with the likelihood of such threats and impact on the business and thereby, deploy controls commensurate to the criticality.
- Portfolio Managers should also encourage its third-party service providers, if any, such as Custodians, Brokers, Distributors, etc. to have similar standards of Information Security.

### **Protection**

#### **Access Controls**

- No person by virtue of rank or position should have any intrinsic right to access confidential data, applications, system resources or facilities.
- Any access to Portfolio Manager's systems, applications, networks, databases, etc., should be for a defined purpose and for a defined period. Portfolio Manager should grant access to IT systems, applications, databases, and networks on a need-to-use basis and based on the principle of least privilege.
- Such access should be for the period when the access is required and should be authorized using strong authentication mechanisms.
- Portfolio Manager should implement strong password controls for users' access to systems, applications, networks and databases. Password controls should include a change of password upon first log-on, minimum password length and history, password complexity as well as maximum validity period. The user credential data should be stored using strong and latest hashing algorithms.

- Portfolio Managers should ensure that records of user access are uniquely identified and logged for audit and review purposes. Such logs should be maintained and stored in encrypted form for a time period not less than two (2) years.
- Portfolio Managers should deploy additional controls and security measures to supervise staff with elevated system access entitlements (such as admin or privileged users). Such controls and measures should inter-alia include restricting the number of privileged users, periodic review of privileged users' activities, disallowing privileged users from accessing systems logs in which their activities are being captured, strong controls over remote access by privileged users, etc.
- Account access lock policies after failure attempts should be implemented for all accounts.
- Employees and outsourced staff such as employees of vendors or service providers, who may be given authorized access to the Portfolio Manager's critical systems, networks, and other computer resources, should be subject to stringent supervision, monitoring, and access restrictions.
- Two-factor authentication at log-in should be implemented for all users that connect using online/ internet facility.
- Portfolio Managers should formulate an Internet access policy to monitor and regulate the use of internet and internet-based services such as social media sites, cloud-based internet storage sites, etc.
- Proper 'end of life' mechanism should be adopted to deactivate access privileges of users who are leaving the organization or whose access privileges have been withdrawn.

#### Physical Security

- Physical access to the critical systems should be restricted to minimum. Physical access of outsourced staff or visitors should be properly supervised by ensuring at the minimum that outsourced staff or visitors are accompanied at all times by authorized employees.
- Physical access to the critical systems should be revoked immediately if the same is no longer required.
- Portfolio Managers should ensure that the perimeter of the critical equipment rooms is physically secured and monitored by employing physical, human and procedural controls such as the use of security guards, CCTVs, card access systems, mantraps, bollards, etc. where appropriate.

#### Network Security Management

- Portfolio Managers should establish baseline standards to facilitate consistent application of security configurations to operating systems, databases, network devices, and enterprise mobile devices within the IT environment. The Portfolio Manager should conduct regular enforcement checks to ensure that the baseline standards are applied uniformly. The checks should be done at least once in a year.
- Portfolio Managers should install network security devices, such as firewalls as well as intrusion detection and prevention systems, to protect their IT infrastructure from security exposures originating from internal and external sources.
- Anti-virus software should be installed on servers and other computer systems. Updation of anti-virus definition files and automatic anti-virus scanning should be done on a regular basis.

#### Security of Data

- Data-in motion and Data-at-rest should be in encrypted form by using strong encryption methods such as Advanced Encryption Standard (AES), RSA, SHA2, etc.

- Portfolio Managers should implement measures to prevent unauthorized access or copying or transmission of data / information held in contractual or fiduciary capacity. It should be ensured that confidentiality of information is not compromised during the process of exchanging and transferring information with external parties.
- The information security policy should also cover use of devices such as mobile phone, faxes, photocopiers, scanners, etc. that can be used for capturing and transmission of data.
- Portfolio Managers should allow only authorized data storage devices through appropriate validation processes.

#### Hardening of Hardware and Software

- Only a hardened and vetted hardware / software should be deployed by the Portfolio Managers. During the hardening process, Portfolio Managers should inter-alia ensure that default passwords are replaced with strong passwords and all unnecessary services are removed or disabled in equipments/software.
- All open ports which are not in use or can potentially be used for exploitation of data should be blocked. Other open ports should be monitored and appropriate measures should be taken to secure the ports.

#### Application Security and Testing

- Portfolio Managers should ensure that regression testing is undertaken before new or modified system is implemented. The scope of tests should cover business logic, security controls and system performance under various stressload scenarios and recovery conditions.
- Patch Management
- Portfolio Managers should establish and ensure that the patch management procedures include the identification, categorization and prioritization of security patches. An implementation timeframe for each category of security patches should be established to implement security patches in a timely manner.
- Portfolio Managers should perform rigorous testing of security patches before deployment into the production environment so as to ensure that the application of patches do not impact other systems.
- Disposal of systems and storage devices
- Portfolio Managers should frame suitable policy for disposals of the storage media and systems. The data / information on such devices and systems should be removed by using methods viz. wiping / cleaning / overwrite, degauss and physical destruction, as applicable.

#### Vulnerability Assessment and Penetration Testing (VAPT)

- Portfolio Managers shall carry out periodic VAPT, inter-alia, including critical assets and infrastructure components like servers, networking systems, security devices, load balancers, other IT systems pertaining to the activities done as Portfolio Manager, etc., in order to detect security vulnerabilities in the IT environment and in-depth evaluation of the security posture of the system through simulations of actual attacks on its systems and networks.
- Portfolio Managers shall conduct VAPT at least once in a financial year. However, for the Portfolio Managers, whose systems have been identified as “protected system” by National Critical Information Infrastructure Protection Centre (NCIIPC) under the Information Technology (IT) Act, 2000, VAPT shall be conducted at least twice in a financial year.

- Further, all Portfolio Managers shall engage only Indian Computer Emergency Response Team (CERT-In) empanelled organizations for conducting VAPT.
- The final report on said VAPT shall be submitted to SEBI after approval from Technology Committee of respective Portfolio Manager, within 1 month of completion of VAPT activity.
- Any gaps or vulnerabilities detected shall be remedied on immediate basis and compliance of closure of findings identified during VAPT shall be submitted to SEBI within 3 months post the submission of final VAPT report.
- In addition, Portfolio Managers shall perform vulnerability scanning and conduct penetration testing prior to the commissioning of a new system which is a critical system or part of an existing critical system.

### **Monitoring and Detection**

- Portfolio Managers should establish appropriate security monitoring systems and processes to facilitate continuous monitoring of security events and timely detection of unauthorized or malicious activities, unauthorized changes, unauthorized access and unauthorized copying or transmission of data / information held in contractual or fiduciary capacity, by internal and external parties. The security logs of systems, applications and network devices should also be monitored for anomalies.
- Further, to ensure high resilience, high availability and timely detection of attacks on systems and networks, Portfolio Managers should implement suitable mechanism to monitor capacity utilization of its critical systems and networks.
- Suitable alerts should be generated in the event of detection of unauthorized or abnormal system activities, transmission errors or unusual online transactions.

### **Response and Recovery**

- Alerts generated from monitoring and detection systems should be suitably investigated, including impact and forensic analysis of such alerts, in order to determine activities that are to be performed to prevent expansion of such incident of cyber-attack or breach, mitigate its effect and eradicate the incident.
- The response and recovery plan of the Portfolio Manager should aim at the timely restoration of systems affected by incidents of cyber-attacks or breaches. Portfolio Managers should have Recovery Time Objective (RTO) and Recovery Point Objective (RPO) not more than 4 hours and 30 minutes, respectively
- The response plan should define responsibilities and actions to be performed by its employees and support or outsourced staff in the event of cyber-attacks or breach of cyber security mechanism.
- Any incident of loss or destruction of data or systems should be thoroughly analyzed and lessons learned from such incidents should be incorporated to strengthen the security mechanism and improve recovery planning and processes.
- Portfolio Managers should also conduct suitable periodic drills to test the adequacy and effectiveness of response and recovery plan.

### **Sharing of information**

- All cyber-attacks, threats, cyber-incidents, and breaches experienced by Portfolio Managers shall be reported to SEBI within 6 hours of noticing/ detecting such incidents or being brought to their notice about such incidents. The incident shall also be reported to CERT-In in accordance with the

guidelines/ directions issued by CERT-In from time to time. Additionally, the Portfolio Manager, whose systems have been identified as “protected system” by NCIIPC, shall also report the incident to NCIIPC. The quarterly reports containing information on cyber-attacks, threats, cyber-incidents, and breaches experienced by Portfolio Manager and measures taken to mitigate vulnerabilities, threats and attacks including information on bugs/ vulnerabilities/ threats that may be useful for other Portfolio Managers shall be submitted to SEBI within 15 days from the quarter ended June, September, December and March of every year. The above information/ reports shall be shared through the dedicated e-mail ids: vapt\_reports@sebi.gov.in and cybersecurity\_pms@sebi.gov.in

- Such details as are felt useful for sharing with other Portfolio Managers in masked and anonymous manner shall be shared using mechanism to be specified by SEBI from time to time.

### **Training**

Portfolio Managers should conduct periodic training programs to enhance awareness level among the employees and outsourced staff, vendors, etc. on IT / Cyber security policy and standards. Special focus should be given to build awareness levels and skills of staff from non-technical disciplines. The training program should be reviewed and updated to ensure that the contents of the program remain current and relevant.

### **Periodic Audit**

Portfolio Managers shall arrange to have its systems audited on an annual basis by an independent CISA / CISM qualified or CERT-IN empanelled auditor to check compliance with the above areas and shall submit the report to SEBI along with the comments of the Board or equivalent body of Portfolio Manager within three months of the end of the financial year.

### **Vendors or Service Providers**

Portfolio Managers have outsourced many of their critical activities to different agencies / vendors / service providers. The responsibility, accountability and ownership of those outsourced activities lies primarily with Portfolio Manager.

Therefore, Portfolio Manager have to come out with appropriate monitoring mechanism through clearly defined framework to ensure that all the requirements as specified in this circular is complied with. The periodic report submitted to SEBI should highlight the critical activities handled by the agencies and to certify the above requirement is complied.

## Lesson 6- Data Analytics and Law

### Research Case of Network Analysis in Law<sup>40</sup>

Court proceedings and its records are interesting for the legal historian, specifically from a perspective of law and its development over the centuries. Such cases are commonly analyzed by intensive reading and note-taking and by identifying commonalities, differences and relationships between documents or elements of documents.

We use these cases to explore whether human analysis can be improved, or at least complemented, by applying network analysis. The latter is a computer science method that allows for the mapping, measuring and visualising of relationships between individuals, groups and other types of information.<sup>41</sup> In this form of analysis, nodes are connected through edges, with the nodes being individuals, groups or information, and the edges being used to link the nodes. By treating court decisions as nodes, and linking the allegations in those cases to legislation and to other cases or scholarly work, network analysis can create a citation network that signals how information flows or has flown, and the extent to which certain nodes in the network are authoritative.

Network analysis has been used for several purposes in the legal field:

- for analyzing criminal behaviour and terrorist networks;
- for finding authoritative cases at courts; and
- for examining legal social networks, networks of statutes and regulatory codes and patent citations.

Volkaert<sup>42</sup> argues that network analysis can be both conceivable and useful in legal history. His recent article provides an overview of research in digital legal history using network analysis and focusing on case citation networks and what he refers to as ‘digital-dogmatic legal history’. According to Volkaert, network analysis can complement dogmatic and contextual legal history, although qualitative juridical interpretations for understanding law remain necessary. By applying network analysis to a selected number of cases of the Court of Friesland, we further explore its potential for legal history research purposes.

### *Recovery from a third party*

For the purposes of the examination, three civil court records with similar cases were selected dealing with the same legal question. Two of these cases could be joined by close reading the court records, while the third was found in a footnote in one of the other case studies. The facts in these three cases were broadly similar in that all three involved an object being sold at an auction. In the first two cases, the object was a black mare, whereas in the third case it was a red spotted cow. All three objects sold were encumbered with a mortgage and all three buyers failed to pay the purchase price, even after being reminded. The auctioneer

---

<sup>40</sup> Reproduced from Hylkje De Jong and Gijs Van Dijck (2022) Network analysis in legal history: an example from the Court of Friesland, The Brill. Available at [https://brill.com/view/journals/lega/90/1-2/article-p250\\_9.xml?language=en](https://brill.com/view/journals/lega/90/1-2/article-p250_9.xml?language=en)

<sup>41</sup> J.H. Fowler et al., Network analysis and the law: measuring the legal importance of precedents at the U.S. Supreme Court, *Political Analysis*, 15 (2007), p. 324-325. See also M.G.H. Schaper, A computational legal analysis of acte clair rules of EU law in the field of direct taxes, *World Tax Journal*, 6 (2014), p. 77 and 80, which provides references.

<sup>42</sup> F. Volkaert, OK computer? The digital turn in legal history: a methodological retrospective’, *Tijdschrift voor Rechtsgeschiedenis*, 89 (2021), p. 1-46, especially p. 37 et seq

who had sold the object subsequently had to recover it from a third party. In all three cases, the latter refused to surrender the object, claiming that it had been sold to him in a legally valid way and that he was therefore an (unassailable) possessor in good faith. Each time, the corresponding legal question was whether the security right (i.e. the mortgage) was valid only if the object was still with the debtor. Or could it also be valid and invoked if the object had been sold to a third party? In other words: did the security right include a right of pursuit, and could the auctioneer recover the object from the possessor in good faith?

Although the facts in the three cases were largely the same, the conditions of the sales were not. In the first case, the auctioneer had added the auction condition *clausula constituti* (a clause from respective constitution) and two sureties, which the plaintiff initially failed to call upon. As a result, and as far as we can reconstruct, the claim was rejected by the court. In the second case (, the auction condition *clausula constituti* was not added, but a specific mortgage was taken out, and there was no surety. Here, it would appear, the security right included the right of pursuit. In the final judgment, the defendant was ordered to hand over the black mare or pay the purchase price to the plaintiff (the auctioneer). The conditions in the third case were the same as in the second case, with the exception of the mortgage. In this case, the mortgage was not a specific mortgage, but a general one, which implied the privilege of the right of eviction. The plaintiff should, therefore, have first sued the non-paying buyer, which he had neglected to do. The Court of thus rejected the claim.

### *Simple interrelationships*

Both the second and third case contains references to one of the preceding cases. In his reply, the plaintiff in the second case, copied 26 articles – the claim, the reply etc. were enumerated – verbatim from the first case. Indeed, he explicitly mentioned this first case at the end of his reply. In the third case, the plaintiff, copied 11 articles verbatim from the second case. These articles also happened to correspond with articles in the first case, although the judgement mentioned only the second case. The three lawyers would appear to have considered their cases to be similar and may have thought they could benefit from the earlier case(s). This interrelationship between the cases was found coincidentally, through close reading. New questions arise from this finding, including how did the lawyers acquire procedural documents from the other cases? Did they have access to them in some way? Was it common to refer verbatim to articles from other court cases? Interestingly, and even without going into the cases in depth, we can also identify another simple interrelationship: the auctioneers from the first two cases and the red spotted cow from the third case all came from a different locational background. Did the lawyers then work together? Did they exchange procedural documents? Linking more cases of a similar nature could provide new answers to questions about legal practice in the early modern period.

Problematic in the study of court records is that it takes a long time to identify allegations in the text and to find relationships between them. One has to be both conscientious and fortunate to recognize interrelationship between litigations. Moreover, based on the sample used for the present study it is hard to draw conclusions. And although the interrelationships mentioned in the three cases studies here were easy to recognize, recognition will be more difficult where the numbers of entities are higher.

### ***Relations between references: Roman law, customary law and case law***

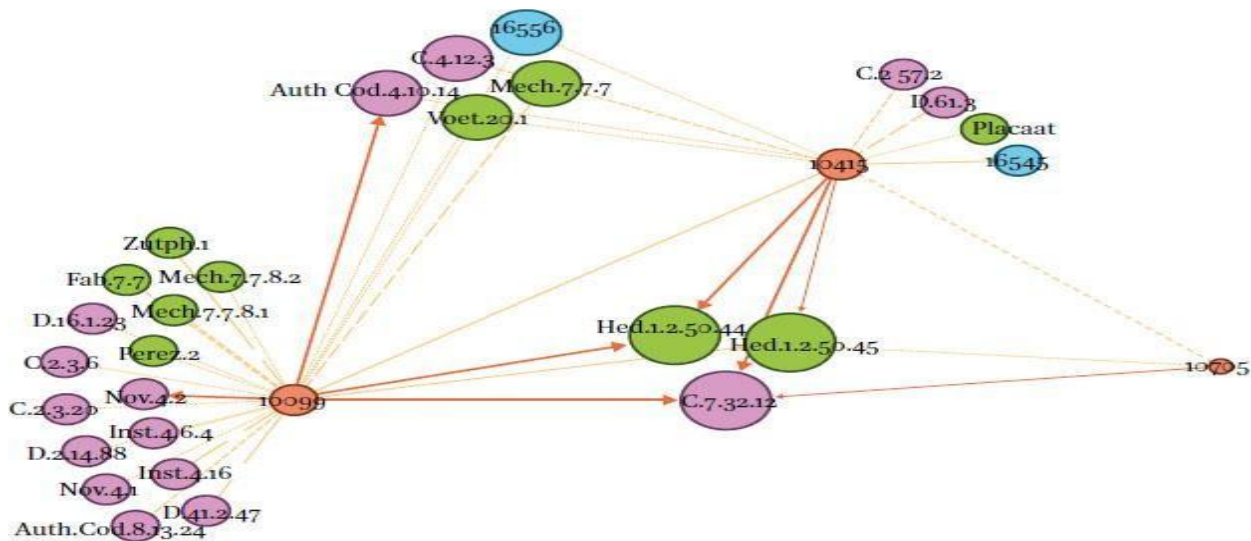
Since the facts and the legal questions in the three cases under consideration are similar, it would not be surprising if the references to the sources also prove to be similar. And, indeed, this turned out to be true. The three cases contain a total of 55 references; of these, 30 were unique references, not including the two references to the other two cases studied here. There is thus an overlap: more than once, the lawyers used the same reference. It is difficult to identify patterns of references through close reading. Instead, therefore, we labelled the nodes (i.e. information entities) and analysed the relationships between them by using network analysis. Before applying this analysis, however, we first had to categorise the various sources to which the allegations referred, given that conclusions can only be drawn on well-defined entities.

For this case study, we distinguished three categories of references, defined more or less by content, Roman law (15 times)<sup>25</sup>, customary law (10 times) and case law (5 times). The three cases are separated from these categories. We are aware that this categorisation is not exhaustive and can be more accurately expanded in future studies, focusing more on the defining of the information entities. Some shortcomings arising from the use of inadequate definitions are that the legal commentaries and works on Roman-Frisian law were classified – for the sake of convenience – under customary law. We also did not take the classification of the use of allegations into consideration, for example, are they copied or are they used by analogy? In addition, no distinction was made between data pertaining to the plaintiff and data pertaining to the defendant. The extent to which references were used at different stages in the legal proceedings was also neglected. However, the three categories chosen were considered sufficient for the purposes of this article, which sets out only to demonstrate the benefit of network analysis for this dataset.

### ***Visualisation of relations***

Visualising connected nodes leverages humans' perceptual abilities to discover patterns from data associated with nodes and edges. The network data in this article were acquired from external data sources. The network is represented by nodes and edges: the nodes are the relational data such as sources (cases on the one hand, and Roman law, customary law and case law on the other hand), while the edges represent the citations between these nodes. On all occasions, the cases records are the sources because only these records contain references.

The visualisation of the references in the three cases is presented in figure 1. The layout of the network is based on the Force Atlas 2 algorithm<sup>28</sup>, with the three cases illustrated in orange as set out below. As mentioned above, the first case has inventory number 10099 (1716), the second 10415 (1718) and the third 10705 (1720). The figure should be read chronologically, from left to right, with references to Roman law being shown in purple, references to customary law in green and those to case law in blue. The node size depends on the incoming references: the more incoming references, the larger the node size (or, in network analysis terms, the larger the in-degree value). The same applies in respect of the thickness of the arrows: the thicker the arrow, the more often the lawyer referred to the particular source.



What can we generally deduce – despite the limited categories – from the network? The three nodes in the middle are the largest and therefore have the highest number of incoming references. All three cases refer to these fragments. The high (in-degree) centrality of these nodes suggests that these fragments are authoritative in this kind of legal issue. The first case in time (10099) contains the most references, while the second case contains substantially fewer references. This second case refers to the first case, as the third case does to the second one. In its references, the third case is limited to the most important references, while the first two cases have some references in common, as shown at the top left. Both these cases refer to other case law in blue (16556). This case is from 20 December 1687. The second case also refers to other case law, specifically the judgment issued on 1 February 1676 (shown as 16545).

References to Roman law account for 50.0% of the references, those to customary law for 33.3% and those to case law for 6.7%, with the remainder comprising references to either or both of the other two cases. It is not surprising that most of the references are to Roman law, given that the Frisians chose Roman law to be applicable. If customary law could be further specified within the category, for example, of Roman-Frisian law, the reception of Roman law could be calculated more precisely. The more accurate the definitions of information entities are, the more specific the information generated will be. However, qualitative juridical research will continue to be necessary.

### Future of network analysis in legal history

For what other legal questions may network analysis be useful? As well as identifying meaningful relations between entities within a dataset, it could be helpful for combining similar sets of entities. If other court archives in the other countries were to be unlocked, relations between these courts could also be revealed.

Today, entire archives of centuries-old material are available digitally and have been made searchable. Although such initiatives have commonly been undertaken in (digital) history departments, initiatives in the legal domain are under development. Fortunately, important initiatives are taken to change this situation. In, for instance, a pilot study, focusing on legal history, at the Department of Legal Theory and Legal History at VU Amsterdam, 48 metres of archives from the Court of Friesland (1499-1811) are being made accessible. The resultant data will be from 2273 civil cases from the period 1716-1730 (all documents

in manuscript). This will be the first time that such a large amount of historical material from legal practice will be available.

A challenge resulting from the increased availability of data is that identifying relationships between documents or parts of documents become unmanageable if only human analysis is applied. While a citation analysis, as conducted in this article, may be feasible with three cases and around 50 references, it would be impossible to conduct such an analysis with 100, 500 or 2,000 cases (nodes) or references (edges). Computational methods can assist in analysing historical data by, for instance, automatically recognising references in the text. This can then result in more data becoming available metadata; that is, data about the data (e.g. citations). The availability of more digitalised documents in the field of legal history will also allow leveraging of computational methods and techniques for analysing the documents, with network analysis then being used, for instance, to explore relationships between large numbers of cases and between references to and from those cases. However, this type of research requires new (digital) skills and implies a transformation, at least in part, of academic research in the sense that the very nature and scope of historical research will change. Moreover, although promising, network analysis has its limitations. For example, particularly in large networks it becomes possible to group nodes (e.g. decisions, cases, arguments, sources) together based on their position in the network. Several algorithms exist for conducting such community detection, yet there is a lack of clarity as to precisely which algorithm is the most optimal one in which type of network. The same holds for determining the centrality of nodes. In-degree (incoming references) and out-degree (outgoing references) are intuitive measures, but a wide variety of additional measures exist, for instance algorithms that take into consideration the centrality of the nodes where references come from or go to (e.g. HITS, PageRank) or that give more weight to references from or to nodes that are younger or published more recently compared to other nodes.

## **Conclusion**

This article discusses three similar cases, in which the legal question at stake was whether security rights (i.e. mortgages) included a right of pursuit. Could the auctioneer recover the object if the buyer failed to pay? The answer to this question depended on the contractual conditions. The lawyers in the three cases from the Court of Friesland appear to have used some of the same references. Network analysis of these references was used to visualise the relationships between these three cases, with the most important references also being made visible. A network can also be customised to suit specific purposes: the more entities (big data) that are defined, the more information that can be generated.

What will the future of network analysis in legal history bring us? Once the 48 metres of civil court records have been labelled, network analysis can be used to expose patterns and trends that cannot be observed by the naked eye, including, for example, relations between legal problems, geographical locations, lawyers and clients. It can then be further leveraged, particularly if references can be detected automatically, to detect relationships between cases, references and actors that cannot be detected by means of human analysis. By comparing legal practice in civil court records in various provinces, or even internationally, network analysis will also make it possible to explore the mode of operation in these courts. This type of research in legal history will then generate new information that will add knowledge to historical legal practice, as well as uncovering information about daily life in early modern history and possibly also leading to a new understanding of the identities of the various provinces.