INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

 ISSN: 2582-6433

EDITORIALTEAM

EDITORS

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur.Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time &Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

 ISSN: 2582-6433

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr.Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

 ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

 ISSN: 2582-6433

THE INFORMATION TECHNOLOGY ACT 2000: A 20TH CENTURY ACT FOR THE 21ST CENTURY DIGITAL INDIA

AUTHORED BY - TANUSKA SARKAR,
ANUSHREE GANGULY & SUBHADIP NANDI,
Students At Government Centre Of Legal Education
(Formerly Law Section, Hooghly Mohsin College, Chinsurah, Hooghly 712101)

Abstract

The Information Technology Act, 2000 in India provides legal recognition for electronic transactions and addresses issues related to cyber crime. However, with the fast changing pace of today's world, the Indian society needs a more comprehensive and stringent law to ensure legal enforceability. The last 25 years have seen a celestial jump when it comes to the Information Technology landscape of India. Unfortunately, Information Technology Act, 2000 fails to be a proper supplement to these changes and remains an obsolete framework in need for severe amendments and even a complete overhaul. From artificial intelligence to cyber warfare, the technological realities and possibilities of 2025 have far surpassed those of 2000.

Introduction

The Indian subcontinent is a varying place of commerce where crores of transactions take place every single day as of 2025. Digital India which was once a dream for a majority of Indians is now a reality in which we are not living but thriving and expanding. In this advanced era where technology acts as a bone marrow for the functioning of any country, it is quintessential to have structured regulations and monitors whose sole duty is to ensure a smooth and safe digital journey.

The Government of India had initiated the roadmap of Digital India back in 2015 whereby India was shown a vision of transformation of Bharat into a digitally empowered society. With the introduction of BHIM UPI, this vision took a shape. By 2025 India saw the evolution of a one-dimensional VAT system of tax into a more synchronised central tax network called GST Network.

 ISSN: 2582-6433

In 2018, the government launched PMGDISHA which stands for Pradhan Mantri Gramin Digital Saksharta Abhiyaan - a scheme which aimed to provide digital literacy in rural areas. During 2020, when Covid had halted almost all of mankind, Digital India came to the rescue by creating the Arogya Setu app which provided COVID related critical information in real time. India revolutionised its own homemade digital transfer system to such a point that France implemented UPI in their country. Today any person can buy Eiffel tower tickets using UPI[1]. During the Financial Year 2023-24, the Reserve Bank of India reported 11,600 crore transactions in India being done using UPI which valued at Rs 2400 crore.[2]

Research Problems and Objectives

It is safe to say that India has steadily kept up with the fast-paced digitisation and has invested in significant infrastructure to keep doing so in the future.

This paper aims to answer the following questions:

- What is the current state of legal regulatory framework in India?
- Has India also developed its legal regulatory framework to cater to the vision of Digital India?

Research methodology

This paper uses a comparative analysis of the existing legal framework of India related to Information Technology Laws and the required legal framework for Digital India and then comments on the validity of the current legal framework.

Current State of legal regulatory framework in India?

Friedrich Carl von Savigny used to believe that law grows with the growth of society, strengthens with the strength of society and finally dies when the society loses it existence. Using this theory, in a realistic world India should have modern laws made at par with modern changes when it comes to the digital aspect.

To understand whether India has achieved such legal framework, we need to determine the existing framework of India with reference to digital laws.

[1] Press-Release-UPI-is-Now-Accepted-in-France https://www.npci.org.in/PDF/npci/press-releases/2024/Press-Release-UPI-is-Now-Accepted-in-France.pdf
[2] Ministry of Finance https://www.pib.gov.in/PressReleasePage.aspx?PRID=1988370

 ISSN: 2582-6433

In the year 2000 a group of Parliament Members passed a bill which was signed by the then Minister of Information Technology on May 9. This bill became the Information Technology Act, 2000. The IT Act of 2000 became a major milestone in the legal chapter of India.

Importance of Information Technology Act 2000

- This Act legalised the concept of digital signatures in India. Earlier physical signatures were the only norm which was followed in all documentation process but with this Act, a person could now authenticate online contracts, thus encouraging paperless commerce on a large scale. Use of digital signature completely replaced the manual process of postal transmission of documents, forms or contracts.
- Cybercriminals could now be held accountable for various acts committed on the Internet,
- for example, Hacking, Identity Theft, Cyberstalking, Data Theft and even Cyberterrorism. Appropriate penal provisions were provided for the respective crimes.
- This Act safeguarded the interests of common man and protected the privacy of such users
- by data security and providing strict punishments for negligent handling of personal data. Under this Act no entity could store personal data without such person's consent.
- The Government also could now digitise their systems and render various kinds of services online without the physical presence of a citizen. The biggest example of this was e-filling of taxes.
- The IT Act also helped in the storage of electronic records as compared to physical records which could be destroyed. Electronic storage and record keeping got a head start after the commencement of this Act.
- An Appellate Tribunal was formed out of this Act to enforce its provisions and provide damages to aggrieved persons who had been a victim of cybercrimes.

Key Provisions of Information Technology Act 2000[3]		
Section Number	**Description**	**Penalty (If Any)**
4	Legal recognition of electronic	

[3] THE INFORMATION TECHNOLOGY ACT, 2000 https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf

 ISSN: 2582-6433

	records	
5	Legal recognition of electronic signatures	
6	Use of electronic records and electronic signatures in Government and its agencies	
7	Retention of electronic records	
43	Penalty and compensation for damage to computer, computer system, etc.	Compensation for damages to the system owner
65	Tampering documents stored within a computer system	Imprisonment of 3 years OR fine of Rs. 2 lakhs OR BOTH
66	Offences associated with computers or any act outlined in Section 43	Imprisonment of 3 years OR fine that extends to Rs. 5 lakhs OR BOTH
66A	Punishment for sending offensive messages through communication service, etc	Imprisonment for 3 years AND fine
66B	Dishonestly receiving a stolen computer source or device	Imprisonment for 3 years OR fine of Rs. 1 lakh OR BOTH
66C	Identity theft	Imprisonment of 3 years OR fine of Rs. 1 lakh OR BOTH
66D	Cheating by personation	Either imprisonment for 3 years OR fine of Rs. 1 lakh OR BOTH
66E	Invading privacy	Either imprisonment up to 3 years OR fine of Rs. 2 lakhs OR BOTH
66F	Cyber terrorism	Life imprisonment
67	Sending explicit or obscene material in electronic form	Imprisonment of 5 years and a fine of Rs. 10 lakhs

 ISSN: 2582-6433

67A	Sending material containing sexually explicit acts of through electronic means	Imprisonment of 7 years and a fine of Rs. 10 lakhs
67B	Depicting children in sexually explicit form and sharing such material through electronic mode	Imprisonment of 7 years and a fine of Rs. 10 lakhs
67C	Failure to preserve and retain the information by intermediaries	Penalty upto Rs. 25 lakhs
68	Failure to comply orders the Controller	Penalty upto Rs. 25 lakhs
69	Failure to intercept, monitor or decrypt data as per the instructions of the government	Imprisonment for 7 years and a fine
69A	Failure to block public access of any information through computer resource as per the instructions of the government	Imprisonment for 7 years and a fine
69B	Failure to monitor and collect traffic data or information through computer resource for cyber security as per the government notification	Imprisonment for 1 year OR fine of Rs. 1 crore

- Sections like section 4 to 7 help in recognition of electronic signatures and provides safeguard and retention of electronic records.
- Section 43 lists a series of offences (unauthorized access to a computer, unauthorized downloads, computer virus, access denial to users, illegal hacking, destruction of software / hardware without consent) that can be done to a computer system or network for which appropriate penal provisions are stated in Section 66.
- Section 65 onwards of the IT Act 2000, dictates the various kinds of offences and their penal provisions.

 ISSN: 2582-6433

Evolution of digital landscape in India since 2000

- Internet has become a staple part of millions of Indian lives now but this was not the scenario in 2000. According to World Bank Group the percentage of Internet users in India went from 1% in 2000 to 43% in 2020[4]. That is a massive leap towards digitisation which absolutely favours development of Indian society but also means that the bane of Internet would be significantly visible.
- Social media and having a social identity may have been an alien concept in 2000 but by 2020 India had almost 378 million Facebook users which made India the largest community of Facebook users on this planet.[5]
- First Post reported in 2023 that there are only 2 countries on Earth that provided cheaper Internet than India, making India one of the largest populated countries with the cheapest Internet.[6]
- During the 2010s India saw a massive surge in telephones whereby the social norm shifted more towards smartphones and by 2023 there were over 700 million smartphones users reported, which is almost half of the population of this country.[7]
- India has emerged as a massive Information Technology Hub and the next step was the Artificial Intelligence revolution and India has once again outshone itself in that aspect. After creating a 200-billion-dollar IT industry, India hosted a Global Artificial Intelligence Summit in 2025.
- Along with a rise in users of Information technology, India also witnessed a massive spike in cybercrimes. According to a report by Norton almost 30 million Indians were victim to cybercrime and the country lost almost 4 billion dollars in losses.[8]
- India has also unfortunately become the hub of some of the world's biggest scam call centres whereby massive call centres are stablished for the sole purpose of defrauding

[4] Individuals using the Internet (% of population) – India https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=IN
[5] Leading countries based on Facebook audience size as of April 2024 https://www.statista.com/statistics/268136/top-15-countries-based-on-number-of-facebook-users/#:~:text=There%20are%20more%20than%20378,terms%20of%20largest%20population%20worldwide.
[6] Mobile data in India is the third cheapest in the world. https://www.firstpost.com/world/india-has-the-third-cheapest-mobile-data-in-the-world-people-is-us-pay-33x-more-than-indians-12614602.html
[7] From Discard to Demand: The Growing Popularity of Used Smartphones https://blogs.idc.com/2024/10/09/from-discard-to-demand-the-growing-popularity-of-used-smartphones/#:~:text=State%20of%20the%20India%20Smartphone,of%20the%20new%20smartphone%20market.
[8] India: Promoting internet safety amongst 'netizens' https://www.unodc.org/southasia/frontpage/2012/May/india_-addressing-the-rise-of-cybercrime-amongst-children.html

 ISSN: 2582-6433

foreign citizens which reportedly generated 38 million dollars of stolen money.

India is thus wielding a double-edged sword when it comes to digital literacy and empowerment. On one hand the Government of India is pouring millions into Information technology, while on the other hand due to lack of strict regulations, cybercrimes are also rising.

Inadequacy of the Information Technology Act 2000.

The Information Technology (IT) Act, 2000 in India was a historic law enacted to render legal recognition to electronic commerce, digital signatures, and to address cybercrimes of all sorts. At a time when the internet was still in its infancy in India, the Act represented a progressive step toward embracing digital transformation. The last 25 years saw a celestial jump when it comes to Information Technology landscape of India. Unfortunately, Information Technology Act 2000 fails to be a proper supplement to these changes and remains an obsolete framework in need for severe amendments and even a complete overhaul. From artificial intelligence and blockchain to big data and cyber warfare, the technological realities and possibilities of 2025 have far surpassed those of 2000.

The following highlight the ways in which the IT Act, 2000 is grossly outdated in today's digital scenario -

1. IT Act is discordant with today's emerging technologies -

The IT Act does not address many of the technologies that dominate today's digital ecosystem, such as -

- Artificial Intelligence (AI): While the Act addresses data privacy breaches, cheating by impersonation (relevant in case of AI-driven deepfakes) and transmission of obscene material (which can be AI-generated), it contains no provisions for AI accountability, its ethical use, or automated decision-making.
- Blockchain and Cryptocurrencies: Both blockchain and cryptocurrency technologies remain in a legal grey zone, with no regulatory clarity. As such, the IT Act fails to regulate the plethora of issues related to them, such as, phishing attacks, routing attacks, sybil attacks, blockchain endpoint vulnerabilities, among others.
- Internet of Things (IoT): IoT devices present numerous security threats, including weak authentication, insecure data transmission, outdated software, and botnets, among others. These vulnerabilities can lead to data breaches, system compromise, and even

 ISSN: 2582-6433

physical harm. The Act is silent on data security and liability for connected devices in case of data compromises and breaches.

- Cloud Computing: The Act does not explicitly address cloud computing and provides no framework for cross-border data hosting or sovereignty over cloud data. Section 43A, along with the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, provide guidelines for body corporations to ensure proper security practices for protecting sensitive data and information.
- Metaverse and Virtual Reality: Issues like virtual identity, digital property rights, and conduct in immersive environments remain unaddressed in the Act.

2. The IT Act has inadequate Data Protection Provisions -

The IT Act's data protection mechanism mainly found in Section 43A is extremely inadequate by global standards. While it mandates compensation for failure to protect sensitive personal and private data, it lacks key principles like informed consent, purpose limitation, and data minimisation. It also offers no individual rights such as access, correction, or erasure of personal data, and does not create an independent data protection authority. The Digital Personal Data Protection Act (DPDPA), 2023 was made to bridge this gap however the simultaneous operation of both DPDPA and the IT Act causes confusion and creates compliance challenges for entities.

3. Obsolete Definitions and Cybercrime Provisions in the IT Act -

Cybercrimes have evolved far beyond what was envisioned in 2000. While the IT Act covers offences like hacking and phishing, it is ill-equipped to deal with the recent frauds of today such as doxxing, deepfakes, cyberstalking, revenge pornography, online radicalisation and cyber terrorism. Scams in the form of fake job offers, lottery, romance and investment scams, digital arrest frauds, etc., are rampant in today's society. Penalties are often lenient and inconsistent, and the Act fails to deter sophisticated cyber criminals. Moreover, procedural inadequacies limit law enforcement's ability to prosecute such offences effectively. More often than not, cyber bullying, rape threats, hacking and death threats in the form of social media comments go absolutely unnoticed and unpunished.

 ISSN: 2582-6433

4. Problematic Intermediary Liability Framework of the IT Act -

The IT Act initially provided a safe harbour to intermediaries such as social media platforms and websites under Section 79, shielding them from liability for user-generated content if they acted as neutral conduits. However, the IT Rules, 2021, significantly altered this balance by imposing stricter obligations such as appointing grievance redressal officers, proactively removing content and enabling traceability of originators. These rules, often criticised for lacking legislative backing, raise concerns about freedom of speech, platform overreach, and privacy violations.

5. Jurisdiction and Cross-Border Challenges are negotiable -

In an era of globally interconnected networks, cybercrimes often cross international borders. The IT Act offers little in terms of jurisdictional clarity for prosecuting foreign-based cybercriminals, mutual legal assistance for digital evidence, cross-border data transfers and international cooperation. This lack of global integration limits India's ability to participate meaningfully in international cyber law frameworks and treaties. The need for international cooperation and consensus is glaringly obvious to tackle the abnormalities due to extra territorial jurisdiction.

6. IT Act's weak framework for Digital Evidence -

The Act's provisions on investigation and evidence collection are poorly suited to modern needs. Sections 69 and 69B allow for surveillance and data interception, but lack procedural safeguards. Law enforcement lacks training in handling encrypted data and blockchain evidence. Moreover, poor chain-of-custody practices often render digital evidence inadmissible in court. Without reform, prosecution of cybercrimes remains ineffective.

7. Legislative Overlap and Fragmentation -

The digital legal regulations in India is being segmented with multiple overlapping laws, namely, the IT Act, 2000, the Digital Personal Data Protection Act, 2023, the Bhartiya Nyay Samhita (amended for cyber offences), and the Telecom Act, 2023. This patchwork approach creates regulatory uncertainty, compliance burdens, and a chilling effect on digital businesses and civil liberties. A singular Act that will cover all possible offences in today's world is necessary for both punishment and deterrence of criminals.

 ISSN: 2582-6433

8. The Act does not recognise Digital Rights -

The IT Act does not recognise fundamental digital rights such as right to privacy, right to internet access, right to be forgotten, algorithmic transparency and accountability. In a world dominated by AI algorithms, big data profiling, and pervasive surveillance, these omissions are glaring and undermine citizens' constitutional protections. Digital footprint of individuals, their personal and private data are often stored via usage of AI models and visiting websites, thereby unknowingly giving access to otherwise protected data.

Latest Amendments and Additional Laws

- **The 2008 Amendment of Information Technology Act 2000**

This amendment was made keeping in mind the growing dangers of internet and cybercrimes. One of the major elements of the amendment was the introduction of section 66A which was a measure to protect women from vulgar and abusive speech on the internet. 66A allowed the power to arrest any person who has been involved in cyber bullying and intimidation.

This amendment also defined 'cyberterrorism' properly via section 66F. Not only section 66F defined cyberterrorism, it also provided penal clauses to counter such cyber terrorism.

Section 43A was amended as a safeguard for personal data and this section heavily mandated body corporates and companies to properly acquire personal data with authorisation, proper handling of such data, compensation and liability in case of mishandling of such personal data.

- **Shreya Singhal V. Union Of India AIR 2015 SUPREME COURT 1523**

Section 66A was provided for the safeguard of women against online abuse and intimidation, however it was not long when the section was being misused. This led to a landmark case in March 2015 when the Supreme Court questioned the validity of Section 66A of Information Technology Act 2000 and declared that Section 66A was unconstitutionally vague which provided limitless powers to government. Therefore, Supreme Court held Section 66A to be against the Freedom of Speech and Expression, and declared section 66A to be void ab initio. Unfortunately, Section 66A still remains as a legal zombie under which cases are still registered in India.

- **Digital Personal Data Protection Act, 2023**

The DPDP Act was passed to mandate the processing of data that is being collected within and outside the territory of India. The main elements of this Act is to appoint Data Protection

 ISSN: 2582-6433

Officer along with independent data auditors and conduct a Data Protection Impact Assessment. The main focus of DPDP is to the creation of Significant Data Fiduciaries whose primary objective to asses the volume of data and its associated risks of handling. The DPDP Act empowers the citizens of India to have the Right to Information on how their personal data is being stored and collected. A person now has a right to alter or erase such data and also nominate someone else to exercise such rights.

An immediate call for reform of Information Technology Act 2000

- The Information Technology Act 2000 in its 25 years of operation has proven that it is of reactive nature rather than being of preventive nature. India is about to embark on a journey to become a trillion-dollar economy and to achieve that, India has to first secure its online canvas.
- The Information technology Act 2000 no doubt was a turning point for the tech industry in India but there is a huge vacuum for a new, objective and comprehensive set of rules and guidelines for future of Indian Information Technology Industry.
- The desperate need for an overhaul is very evident from the fact that majority of cybercrimes in India are bailable offences which reduces the quantum of punishment. These leads to very few actual convictions under the Act.
- With the advent of cryptocurrencies and faster Internet speeds, internet misusers are harder to track and arrest. The rural areas of India may have been injected with the usage of Internet, however, due to lack of proper safeguarding methods and safe searching, Tier -2 level citizens are constantly prone to cyber-attacks and scams.
- Using the loopholes of existing laws, multinational companies are openly promoting gambling under the false pretext of ‘gaming’ and by showing rewards of financial gains, innocent and naïve citizens are incurring heavy losses.
- India had opened the doors of globalisation much before the advent of this Act and thus in the current scenario, Indians are constantly using foreign applications. Some of these applications gets easy access to personal data and is involved in selling such data for financial gain.
- Artificial Intelligence and Machine Learning are the next major milestones in the journey of mankind and have consumed major sectors like health, education, governance, engineering, etc. With the evolution of AI the dangers of exploitation have never been higher. The Information Technology Act 2000 absolutely fails to

 ISSN: 2582-6433

comprehend such dangers or provide a legal framework about the same.

Conclusion

"Has India also developed its legal regulatory framework to cater to the vision of Digital India?"

India has made a decent attempt to mirror the light-speed evolution of the technology landscape when it came to supplementing laws and rules, however, it has failed to catch up with the societal developments. The existing IT laws are obsolete and feel incomplete and vague. Certain definitions of offences under the Act are not stream lined and are kept unclear. This creates a potential threat for the future of Digital India. Being aware of this problem the Government of India has proposed the Digital India Act which will replace the Information Technology Act 2000. The main focus areas of the Act would be:[9]

1. Regulations on 5G, Internet of Things, Cloud Computing, Blockchain, Metaverse, Cryptocurrency
2. Reclassification of online intermediaries to decentralise the intermediary network instead of one general intermediary
3. Creating proper standards for use of Artificial Intelligence and Machine Learning
4. Regulation of monetisation of content and online advertising.
5. Anti-monopoly rules to break tech companies from creating monopolies in digital space
6. Remove safe harbour immunity causes of the Information Technology Act 2000 for better accountability and liability

[9] What is the Digital India Act? India's Newest Digital Law https://www.upguard.com/blog/digital-india-act#:~:text=Removing%20monopolies%20of%20the%20digital,space%20by%20big%20tech%20companies.