RED LAB™
Rediffusion Consumer Lab

The Digital India Act

Legal Framework for Digital India: Challenges and Opportunities

A lot of the content of this report has been sourced from **www.digitalindia.gov.in**

Prof. Avanindra Chopra
Culture, Customs & Conversations Specialist, Red Lab

EMERGENCE OF DIGITAL INDIA

The emergence of a digital India is duly acknowledged and widely appreciated. All around us, more and more Indians meet digitally, study digitally, work digitally, receive and spend monies digitally, pay their taxes digitally, interact with the government and private companies digitally, order products and services digitally, and so on. Significantly, the **Reserve Bank of India** is planning to issue **Central Bank Digital Currency (CBDC).** It will be referred to as **e₹ (digital Rupee).**

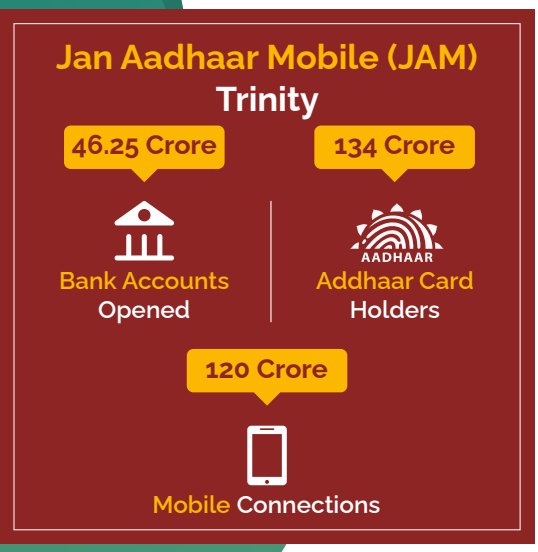
That India is likely to have **900 million** active internet users by 2025, up from around **795 million** as of 2020 comes as no surprise. Strangely, the internet user base in rural areas has been growing faster than in urban India on a year-on-year basis — **4% for urban India** vs **13% growth in rural areas.**

Already, this stupendous growth riding on the ubiquitous 4G networks and inexpensive data plans has enabled the creation of digital platforms and applications that are being used by millions in areas such as health and education, agriculture and industry, commerce and culture, transport and tourism, disaster management and safety, security and surveillance, industry and logistics, social welfare policies and entertainment and what have you.

Digitalisation has ushered in the age of startups as well. India has emerged as the 3rd largest ecosystem for startups globally with over 77,000 **Department for Promotion of Industry and Internal Trade** recognized startups across 656 districts of the country as of August 2022 and this has come largely due to the freedom to build and the ease of access to internet platforms. Moreover, as of Sept 2022, India is home to **107 unicorns** with a total valuation of **$ 340.79 billion.** Out of the total number of unicorns, **44 unicorns** with a total valuation of **$ 93.00 billion** were born in 2021 and **21 unicorns** with a total valuation of **$ 26.99 billion** were born in 2022.

It is believed that the game changer in boosting digitalization has been the success of the near universal **Aadhaar** enrolment. There are **1.34 billion holders** of this unique identification proof s of 30th June, 2022. The Unique Identification Authority of India (UIDAI), claims that the total number of Indian adult population holding Aadhaar has touched **99.9%** and 'use it at least once a month'. Aadhaar facilitates the activation of the all important **SIM** card for a **mobile** phone connection. In fact, it is Aadhaar that has created 'a public digital rail' on which several digital platforms have been built.

As per a **Deloitte** study, India had 1.2 billion **mobile** subscribers in 2021, of which about **750 million** were **smart-phone users,** all on one platform or the other. Latest technology has made it possible for even feature phone users to access



some social media and productivity apps. They can easily ask questions, get directions and even make calls by just using their voice.

The show stealers in this march of digitalisation have been the **JAM trinity (Jan Dhan-Aadhaar-Mobile)** linkage leading to the opening of over **46.25 crore** bank accounts. 56% Jan-Dhan account holders are women and 67% Jan Dhan accounts are in rural and semi-urban areas. **31.94 crore RuPay cards** have been issued to them. About 5.4 crore account holders have received **Direct Benefit Transfer (DBT)** from the Government under various schemes in June, 2022. This has provided vital funding to vulnerable populations. Then there are the Aadhaar based **CoWin Platform** that has delivered over **2 billion jabs,** the Unified Payments Interface (UPI) that boasts of nearly **7 billion transactions** a month, the online **GST** collection system that has been contributing on an average over **1.4 lac crores** a month to the national exchequer, and many more.

It is believed that things will change dramatically with the development of the **Open Network for Digital Commerce (ONDC)** that aims to revolutionize the buyer-seller relationship, the **Account Aggregator framework** and the **Open Credit Enablement Network** that aims to provide credit at bank rates to all and sundry. The recently announced GoI incentive package of **$ 10 billion** to boost semiconductor manufacturing in India will further boost digitalisation.

THE PUSH TOWARDS DIGITAL

Source: www.digitalindia.gov.in

It needs to be noted that earlier the **Ministry of Communication and Information Technology** used to look after the three vital departments of telecom, IT and postal services. The ministry consisted of three departments, viz. **Department of Telecommunications, Department of Electronics and Information Technology (DeitY),** and **Department of Posts.**

In 2016 it was bifurcated into two separate ministries - **Ministry of Communications and Ministry of Electronics and Information Technology (MeitY)** with **DeitY** becoming **MeitY** - a standalone full-fledged ministry responsible for IT policy, strategy and development of the electronics industry. The **DeitY** itself had superseded the **Department of Information Technology** in 2012.

The **Ministry of Communications** continues to remain responsible for telecommunications and postal services.

What's more, the **Telecom Commission,** set up by the **GoI** in 1989 to deal with various aspects of Telecommunications was re-designated as the Digital Communications Commission in 2018, with **'a vision to support India's transition to a digitally empowered economy and society'.**

All these changes capture the shift in strategy and focus of the **GoI** on **digital tech.**

5G SERVICES IN INDIA

And now, with the launch of the next generation **5G services** in India, data speeds are likely to get 30 times faster - increasing **'energy efficiency, spectrum efficiency and network efficiency'.** 5G seeks to provide seamless coverage, low latency and highly reliable communications system.
5G services are further expected to play a major role in achieving the economic goal of making India a **$5-trillion economy** by 2024-25. According to experts, 5G will have a cumulative economic impact of **$1 trillion** by 2035 and can deliver an additional **GDP of $150 billion** for the country, between 2025 and 2040.

PEEYUSH VAISH

Peeyush Vaish, Partner and Telecom Sector Leader, Deloitte India, says that over 75 percent of the subscribers will use smart-phones by 2026 from a sub-70 percent as on date.
"5G-enabled devices will contribute 80 percent to the devices being sold in the year 2026 and Indian consumers will purchase 840 million 5G smart-phones over the next 5 years valued at USD 130 billion. In addition, 5G will fuel an incremental sale of 135 million smart-phone units over the next 5 years," Vaish adds. This will hugely aid the digital push in India.

Deloitte.

DIGITAL INDIA PROGRAMME

And, with the vision of transforming India into a digitally empowered society and knowledge economy, the **GoI** has embarked on the **Digital India** programme since 2015. This flagship programme has identified nine pillars of growth areas, namely Broadband Highways, Universal Access to Mobile Connectivity, Public Internet Access Programme, e-Governance: Reforming Government through Technology, e-Kranti - Electronic Delivery of Services, Information for All, Electronics Manufacturing, IT for Jobs and Early Harvest Programmes. Each of these areas is a complex programme in itself and cuts across multiple Ministries and Departments.

NINE PILLARS OF DIGITAL INDIA

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

Source: www.digitalindia.gov.in

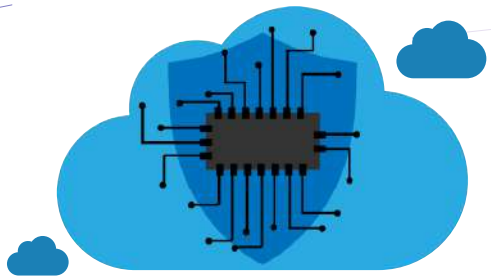
The Digital India programme, earlier coordinated by **DeitY** is now handled by **MeitY,** and implemented by the entire government. The common branding of programmes as Digital India highlights their transformative impact. It is centered on 3 Key Areas:

- Digital Infrastructure as a Utility to Every Citizen
- Governance and Services on Demand
- Digital Empowerment of Citizens

The Government has also committed huge amounts for digital inclusion. Providing high quality connectivity in unconnected areas, revival of **BSNL,** taking optical fiber to all gram panchayats, developing India's own telecom technology stack, and developing telecom manufacturing ecosystem, demonstrate the government's commitment to digital inclusion.

BSNL
Connecting India

THE CHALLENGE — A COMPREHENSIVE LEGAL FRAMEWORK



It is worth bearing in mind that many of the top service, e-commerce, social media intermediaries, telecom providers and internet companies did not exist in 2000 when India passed its first **Information Technology Act.** The basic digital services, taken for granted now were still to be introduced. Online ticketing was first launched by the **IRCTC** only in 2002 and two years later the airlines followed. **Google** opened its first office in India in 2004 but it was just a minor search engine then. **BSNL** commenced its broadband services in 2004. And, the social networking phenomenon took off in India in 2005 with **Orkut,** and **Facebook, (now Meta)** came a year after. **Twitter** came in 2006, **Flipkart** in 2007, **Youtube** in 2008, and **Amazon** and **Instagram** entered the Indian market in 2012. In 2008, **2G spectrum** was allocated followed by **3G** a year after. The **Aadhaar** revolution providing billions a plethora of digital platforms, services and applications began in 2009.

At that time, there was little idea of online financial fraud and other digital crimes or of the upheavals social media could cause and therefore, legislating against such digital offences and crimes of today could not be foreseen. The time

Industry 4.0

when this IT Act was passed was the era when baby steps towards 2G/3G were dreamed of and speeds of 5G and 6G and new technologies that are creating new opportunities for India's socio-economic growth today, like the **Internet of Things, Industry 4.0, M2M Communications, Mobile Edge Computing,** etc., were in the realm of scientific fantasy.

This rapid transition to digitalisation, along with cutting edge technological infrastructure also requires a robust and effective **legal framework** that assures **safe and secure transactions** in the digital world and puts in place universally acceptable guidelines, principles and a vision that guide and empower individuals, businesses and governments in the digital universe.

To achieve the desired goals, cyber specialists state that the **GoI** has to clearly define the jurisdiction of the fresh laws that are being planned in the crucial areas of telecom, information technology and data protection. Two of these have been placed in the public domain as the **Indian Telecommunication Bill, 2022** and the now withdrawn **Personal Data Protection (PDP) Bill, 2019** with the draft of the **Digital India Act** (the new Information Technology Act) being eagerly awaited. The government has to be careful in finalizing these legislations because any "overlap" between provisions will lead to regulatory conflict in the future.

PRIME MINISTER
SHRI NARENDRA MODI

Speaking at a meet of law ministers and law secretaries of states recently, even **PM Narendra Modi** has said that laws need to be be framed simply and in local languages so that common people can comprehend them. The laws also must come with an 'expiry date', indicating how long they will remain in force and claimed that his government has **scrapped 1500 old, obsolete laws.** Something similar must be done with the laws concerning the digital arena. The old obscure laws should be discarded and new laws in sync with changing times adopted.

Now, let's look at some of the key legislations proposed and the issues involved.

INDIAN TELECOMMUNICATION BILL 2022

Telecom provides the entry point into the digital world. In September 2022, the **GoI** notified the **Indian Telecommunication Bill, 2022** for public feedback and comments. Notably, at present India has the world's second largest telecommunication ecosystem with **117 crore** subscribers. Importantly, the telecommunication sector employs more than **4 million** people and contributes about **8%** of the country's **GDP.**

The existing regulatory framework for the telecommunication sector is based on the **British era Indian Telegraph Act** enacted in **1885** and the **Indian Wireless Telegraphy Act** enacted in **1933. The Telegraph Wires (Unlawful) Possession Act** was enacted in **1950.**

The Indian Telecommunication Bill looks to repeal these three legislations and **"restructure the legal and regulatory framework"** in an attempt to revamp both telecom and internet regulations. The stated purpose of the new regulation is to provide greater **protection to consumers' rights and privacy** as it will strengthen the safety and security of the customers.

TRISHEE GOYAL

VIDHI Centre for Legal Policy

Trishee Goyal, a **research fellow** at the **Centre for Applied Law and Technology Research, Vidhi Centre,** writes in **The Hindu** that the current draft of the Bill expands the definition of **"telecommunication services"** to include **over-the-top (OTT)** communication services like **Whatsapp, Telegram, Signal, Messenger, Duo, Google Meet, Snapchat,** etc. This could result in them being subject to the same licensing conditions as telecom service providers like **Airtel, Vodafone** and **Jio** as they too provide features that are akin to those provided by telecommunication services such as voice calls and SMS services. The bill proposes to manage these Over-the-top (OTT) messaging services/platforms based on the **"same service same rules"** premise.

The Bill expands the scope of lawful interception of communications and requires telecom players to identify users by ensuring that **Know Your Customer** norms are followed. It proposes that the identity of the person communicating using any form of telecommunication services shall be available to the user receiving such communication. This would mean that unlike now where only the phone number of the person making the communication is displayed, going forward the name of the person would be displayed too.

To ensure that a user provides correct details, the draft Bill penalises the **person providing wrong identification details with a ₹50,000 fine** and **suspending the operation** of the specific mobile number or barring the person from using the telecom service for a certain duration. The bill creates a **"do not disturb"** register that requires the prior consent of the user for receiving a certain class of messages which are advertising and promotional in nature.

CHAITANYA NETKALAPPA

DH
DECCAN HERALD

Chaitanya Netkalappa, (Deccan Herald) observes that the bill lays down explicit statutory framework and regulatory clarity for the **Central Government** to undertake spectrum assignment. The underlying philosophy is that spectrum assignment should serve the common good and ensure widespread access to telecommunication services. The bill provides for assignment of spectrum primarily through auction. For certain specified functions relating to government and public interest such as defence, transportation and research, the bill provides an enabling framework for assignment of spectrum through administrative process.

The Bill includes provisions covering **spam messages,** and defines norms related to **Internet shutdowns, Right of Way for installation of telecom infrastructure** and **licensing norms** for telecommunication services. It dilutes **TRAI's Recommendatory Powers** as its nod is no longer necessary for issuing a new licence to a service provider.

TRAI

Some professionals have welcomed the bill as they feel that the overall regulation is **'generic and simple'.** They believe that the law will not stifle the innovation aspect and will provide an enabling environment to the new players without asking them to delve into the tough regime of approvals, limits, etc. They feel that as light-touch regulations are proposed, the industry is not apprehensive of over-regulation.

But other industry experts warn that **the bill lacks clarity** on many aspects including consumer privacy and may lead to greater government interference as the draft bill proposes powers to the government to order **internet shutdowns** or **intercept communications** including messages.

THE PERSONAL DATA PROTECTION BILL, 2019

Since **'privacy is a fundamental right of citizens and having a trillion-dollar Digital Economy requires global standard cyber laws',** the government brought in The **Personal Data Protection Bill** in 2019. The bill's preamble identified three key focal points:

- … the right to privacy is a fundamental right and it is necessary to **protect personal data** as an essential facet of informational privacy;
- …. the growth of the **digital economy** has expanded the use of data as a critical means of communication between persons;
- …. it is necessary to create a collective culture that fosters a **free and fair digital economy,** respecting the informational privacy of individuals, and ensuring e**mpowerment, progress** and **innovation** through digital governance and inclusion…

PRS

The aims of the Bill were:

'to provide for **protection of the privacy of individuals relating to their personal data,** specify the flow and usage of personal data, create a relationship of trust between persons and entities processing the personal data, protect the rights of individuals whose personal data are processed, to create a framework for organisational and technical measures in processing of data, laying down norms for social media intermediary, cross-border transfer, accountability of entities processing personal data, remedies for unauthorised and harmful processing, and to establish a Data Protection Authority of India for the said purposes and for matters connected therewith or incidental thereto.'

As explained by **PRS Legislative Research ("PRS")** the bill sought to provide for protection of personal data of individuals, and establish a **Data Protection Authority** for the same. It allowed for categorization of certain personal data such as **financial data, biometric data, caste, religious or political beliefs**, or any other category of data specified by the government, in consultation with the Authority and the concerned sectoral regulator as sensitive personal data. It allowed processing of personal data only if consent was provided by the individual. However, in certain circumstances, personal data could be processed without consent. These included: (i) if required by the **State for providing benefits to the individual,** (ii) **legal proceedings,** (iii) to respond to a **medical emergency.**

Sensitive personal data could be transferred outside India for processing if explicitly consented to by the individual, and subject to certain additional conditions. However, such sensitive personal data should continue to be stored in India. Certain personal data notified as critical personal data by the government could only be processed in India.

The bill was referred to **The JPC (Joint Parliamentary Committee)** that examined the **Bill** and tabled its report in **Lok Sabha** in December 2021. The committee proposed a single law for dealing with both personal and non-personal data. The report suggested moving towards complete localisation of data. There was strong opposition to the provision in the **Bill** that provided the government with powers to give exemptions to its probe agencies from the provisions of the Act. Other objections related to difficulties in compliance that startups would have likely faced, and also because many provisions of the **Bill,**
such as **data localization, hardware authenticity clauses,** and so on, went beyond the ambit of data protection. Provisions over data localisation invited considerable criticism from companies, especially foreign tech companies and the **governments of US** and **Europe** along with **Indian startups.**

ARINDRAJIT BASU

THE CENTRE FOR internet & society

Considering the 81 amendments and 12 recommendations proposed by the **JPC,** the government withdrew the **Bill** in August 2022 and said that it would be replaced with a new bill with a **'comprehensive framework'** and **'contemporary digital privacy laws'.**

Arindrajit Basu, a research manager at the Centre for Internet & Society, India, observes,

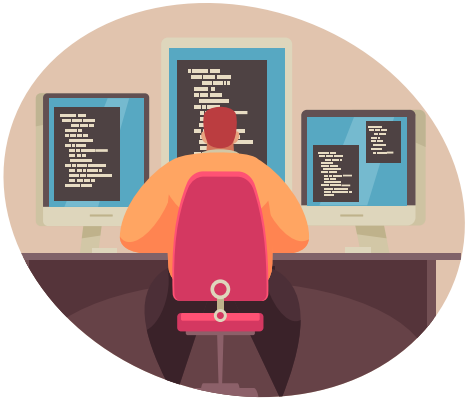
'In fact, the biggest concern about the bill among academics and activists is the exemptions granted to the government for data collection.' He points out that that the phrase **"necessary or expedient"** has replaced the usual **"necessary and proportionate"** phrase recognized as standard in Indian constitutional and international law. He adds, 'Just last year, the right to privacy ruling had stated clearly that any intrusion into the right must be authorized by law, conducted in accordance with procedure established by law, and be necessary and proportionate to the objective being sought. The use of the term **"necessary or expedient"** does not impose an obligation to undertake the balancing act between the intrusion and the objective, thereby augmenting the government's surveillance powers. This leaves a gaping regulatory vacuum around surveillance law in India and fails to adequately protect citizen privacy, as there are no clear rules that govern government use of data.'

JUSTICE
BN SRIKRISHNA

Perhaps the most damning criticism of the **Bill** was by **Justice BN Srikrishna,** who had led the committee that drafted the **Personal Data Protection Bill.** He said the final bill placed in **Parliament,** which allowed the **Centre** to exempt its agencies from some or all provisions, was **"dangerous"** and could turn India into an **"Orwellian State".**

As per latest reports, in the proposed revised version of the **PDP Bill,** that may be released for public consultation in a few weeks, the government is likely to relax provisions on data localisation or cross border flow of data but will ensure that all data belonging to Indian citizens remains available for law enforcement agencies or any other government organisation which is legally entitled to access such data. **Cross-border flow of data** will be permitted as long as the government is able to access the data legally.

INFORMATION TECHNOLOGY ACT, 2000



It was way back in 2000 that the **GoI** brought out the **Information Technology Act.** The aim was to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as **"electronic commerce".** It facilitated electronic filing of documents with the Government agencies and further amended the **Indian Penal Code,** the **Indian Evidence Act, 1872,** the **Bankers' Books Evidence Act, 1891** and the **Reserve Bank of India Act, 1934** enabling such transactions.

This Act was based on the 1997 resolution of the **General Assembly of the United Nations** that adopted the **Model Law** on Electronic Commerce approved by the **United Nations Commission** on **International Trade Law.** The offences included under the Act were:

- Illegal access, the introduction of a virus, denial of services, causing damage and manipulating a computer, computer system or computer network.
- Tampering, destroying and concealing computer code.

- Acts of hacking leading to wrongful loss or damage.
- Acts related to publishing, transmission or causing publication of obscene/ lascivious in nature.

Experts feel that the **IT Act, 2000,** was primarily meant to be a legislation to promote e-commerce. It addressed issues pertaining to **electronic documents, e-signatures,** and **authentication** of those records. It also sought to establish **Cyber Regulations Appellate Tribunals** within the country to adjudicate on these matters. But studies of the **IT Act, 2000** point out that the goals were really not met. **Cybercrime** as a term was not defined in the act. The act only dealt with few instances of computer-related crimes.

THE FLAWS OF THE IT ACT, 2000

Though the **GoI** went on to establish the first and the only **Cyber Appellate Tribunal (CyAT)** in New Delhi in 2006, its failure to appoint a **Chairperson** since 2011 has made the tribunal non-functional. The **non-working of the tribunal** has led to cyber cases being filed in the courts that are already facing huge pendency issues. Along with a conflict of jurisdiction, **the delay is leading to problems** in implementation of the Act.

It is also argued that the quantum of punishment for cyber offences under the **Act** is not adequate and cyber crimes need to be made non-bailable offenses. Furthermore, the **IT Act** does not cover a majority of crimes committed through mobiles. It is felt that there is a **lack of expertise** in the security agencies to tackle cybercrimes. **Cybercrimes** can only be curbed by a highly trained cyber expert force. Cyber crime cannot be handled by untrained police officers.

SUBHAJIT BASU

UNIVERSITY OF LEEDS

DR. PAVAN DUGGAL

PAVAN DUGGAL ASSOCIATES

According to **Subhajit Basu, an Associate Professor at the University of Leeds** and **Prof Richard Jones of Liverpool John Moores University,** the **IT Act, 2000** is a strange mixture of provisions that other jurisdictions have chosen to legislate separately. The Act is in no way comprehensive and while dealing with many of the major issues in e-commerce it is lacking in provisions relating to: **taxation issues arising out of e-commerce;** intellectual property rights such as **digital copyright issues, trademarks, patents; domain name registration policy, disputes and cyber-squatting; privacy and data protection issues; junk mail and spamming; guidelines for content, technological standards** and **electronic payments.**

Dr. Pavan Duggal, an expert and authority on Cyber Law has argued that the **Act is a toothless legislation** which has not been completely effective in issuing **penalties** or **sanctions against perpetrators** who choose to misuse the reach of cyberspace.

INFORMATION TECHNOLOGY AMENDMENT ACT, 2008

To address some of the main concerns a major amendment to the **IT Act, 2000** was made in 2008 through the **Information Technology Amendment Act, 2008.** The highlights of the amendments were the introduction of the controversial **Section 66A** which penalized sending **"offensive messages".** It introduced **Section 69** too, which gave authorities the power of **"interception or monitoring or decryption of any information through any computer resource".** Additionally, it introduced provisions addressing - **pornography, child porn, cyber terrorism and voyeurism.**

Some of the main offences under the Information Technology Amendment Act, 2008 are the following:

- Tampering with Computer Source
- Punishment for sending offensive messages through communication service, etc.
- Punishment for dishonestly receiving stolen computer resource or communication device
- Punishment for identity theft
- Punishment for cheating by personation by using computer resource

- Punishment for violation of privacy
- Punishment for publishing or transmitting obscene material in electronic form
- Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form
- Punishment for cyber terrorism
- Power to authorize to monitor and collect traffic data or information through any computer resource for Cyber Security
- Penalty for misrepresentation
- Breach of confidentiality and privacy
- Punishment for Disclosure of information in breach of lawful contract
- Penalty for publishing electronic Signature Certificate false in certain particulars
- Publication for fraudulent purpose

THE FALLOUT OF THE INFORMATION TECHNOLOGY AMENDMENT ACT, 2008

Even though the amendments and the multiple rules framed there under sought to address various issues, experts feel that concerns regarding **transparency, cyber security, spamming, phishing, data protection in internet banking, privacy protection, identity theft, cyber war, cyber stalking, cyber fraud, chat room abuse, theft of internet hours, copyright and trademark violations, gaming, crypto currency, social media** and many more remain. Some sections of the amendments have led to heated debate in the public sphere.

Major pieces of secondary and subordinate legislation like the **Information Technology (Intermediaries Guidelines) Rules, 2011,** the **Information Technology Intermediary Guidelines (Amendment) Rules, 2018 and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021** have been notified to make basically social media intermediaries accountable. These Rules have been framed to curb users from engaging in online material which is **paedophilic, pornographic, hateful, racially** and **ethnically objectionable, invasive of privacy,** etc., and to prevent **mob lynchings** spurred by fake news and rumours and messages circulated on social media platforms.

Intermediaries are supposed to observe due diligence while discharging their duties, and also observe such other guidelines as prescribed by the **Central Government.** The changes also require online platforms to break end-to-end encryption in order to ascertain the origin of messages. But making platforms share more information could prove counterproductive in a country where the citizens still do not have a data privacy law to guard themselves against excesses committed by the government or the intermediaries.

In 2015, the **Supreme Court of India** declared **Section 66A** as unconstitutional. The court said that it **"arbitrarily, excessively and disproportionately invades the right of free speech"** provided under **Article 19(1)** of the Constitution of India. But the Court turned down a plea to strike down **Sections 69A** and **79 of the Act,** which deal with the procedure and safeguards for blocking certain websites.

Section 69 allows for the interception or monitoring or decryption of any information. But, a 1996 **Supreme Court** verdict states that the government can tap phones only in case of a **"public emergency".** But, there is no such restriction under Section 69.

In 2018, the **Ministry of Home Affairs** cited Section 69 when it issued an order authorising ten central agencies to intercept, monitor, and decrypt **"any information generated, transmitted, received or stored in any computer."** While some claim this to be a violation of the fundamental right to privacy, the Ministry has claimed its validity on the grounds of national security. Data privacy rules too require firms

to obtain written permission from customers before collecting and using their personal data.

In November 2020, the **GoI** brought **over-the-top ('OTT')** platforms such as **Netflix, Amazon Prime** and others under the regulation of the **Ministry of Information and Broadcasting ('MIB'),** thereby subjecting them to censorship standards set by the Government.

The government is also likely to publish the final draft of the updated **Information Technology (Intermediary Guidelines** and **Digital Media Ethics Code) Rules, 2021** soon. A major update of the Rules will be the government setting up the grievance appellate committees **(GACs)** to address concerns of users against social media platforms.

Over the years, **cyber experts** have been highlighting the shortcomings in the **IT Act, 2000** and its subsequent amendments and rules. Too many rules and amendments have led to a lot of confusion in implementing the Act. And many activists and affected parties have been fighting in the courts for redressal of their grievances. Various petitions have been filed challenging the rules and interim stays from courts and judgments have added to the quagmire, making implementation of the Act hard and tricky. Bitter court battles between the government and social media giants such as **Twitter** and **Whatsapp** have vitiated the atmosphere.

TOWARDS THE DIGITAL INDIA ACT - THE NEW INFORMATION TECHNOLOGY ACT

RAJEEV CHANDRASHEKHAR

So, to address the problems arising from the inadequacies of the **Information Technology Act, 2000** and its subsequent amendments/rules, the **GoI** plans to introduce the **Digital India Act (DIA) (the new Information Technology Act)** in the next few months. This has been stated amongst others, by the **minister of state for electronics and information technology, Rajeev Chandrashekhar.** He has said that India will replace the **IT Act, 2000** with a **Digital India Act,** comprising a modern framework of laws and rules that will act **'as catalysts for innovation and protecting citizen's rights'.** The new legal framework will be attuned to the realities of the 21st century to make India succeed in the **'techade'.**

The new regulation hopes to cover the entire digital ecosystem, from social media platforms, **OTT** platforms, and online apps, to the **metaverse** and **blockchain-based crimes** or offences and to target misinformation and incitement to violence. Further, with India set to build a **USD 300 billion electronics manufacturing industry** by 2025-26 from present levels of USD 75 billion, making it a preferred partner in global supply chains, it becomes imperative to have effective legislation in place soon. **The Digital India Act,** being an umbrella act will address issues ignored by the earlier Act. It will cover all things digital and will feature specific **guidelines for women and children's safety online.** It will even address situations where an avatar bullies or sexually abuses another avatar in the **metaverse.**

Welcoming this, the **Tata Sons Chairman N Chandrasekaran** has said the upcoming Digital India Act is **"necessary"** as it has been over two decades since the IT Act was promulgated and the technology landscape has changed since then.

ASHWINI VAISHNAW

"I think the Digital India Act is necessary because so much has changed over the last couple of decades since the original IT Act was put in place," Chandrasekaran said, addressing the annual general meeting of TCS virtually. **"I am glad that the government is engaged and developing a participative approach to develop the Digital Act which is an important thing, especially there are new issues like privacy and other aspects that will come into this (new) Act,"** he added.

The **Union minister** in the **electronics and information technology, Ashwini Vaishnaw,** has stated that the government is looking to make the online world more accountable for published items through the proposed new version of the **Data Protection Bill** and the amendment to the **IT Act 2000,** known as the **Digital India Act.** The government will in addition be floating a new telecom bill, and has requested stakeholders to provide their suggestions on the draft.

Thus the need for comprehensive laws is well accepted. The government proposes to have new rules, regulations and laws rolled out in the next few months and this will be done with consideration to all the involved stakeholders and countries. **The government aims to build good legislation, rules and framework** and an enabling environment which will ensure India's success in the coming decade.

ANKITA SINGH

It is hoped that the new law will empower the government to effectively deal with a **Twitter** handle or **Facebook** page if it's found to be spreading misinformation or inciting violence. Besides, it may include measures to regulate content on over-the-top (OTT) video streaming platforms such as **Netflix** and **Amazon Prime Video.** With even the draft of the proposed Digital India Act yet to see the light of the day, there are reports that top tech multinationals like **Google, Facebook, Twitter, Amazon** and **Facebook** are studying the impact of the changing regulations due to the upcoming legislation on their operations. Companies have engaged experts to analyse the upcoming regulation, look out for any likely conflict, and prepare themselves accordingly.

Ankita Singh, partner at law firm A&P Partners says, "The regulatory landscape in India is changing very fast on the digital front and the big tech multinationals are getting impact analysis done on how this would affect their operations and revenues. In some cases, these companies even want to create structures or insulate their data or other intellectual properties, as not doing so could have global repercussions for them."

SIDDHARTH VISHWANATH

pwc

Siddharth Vishwanath, partner at PwC India adds, "The expected DIA is likely to make things more onerous for big techs... Stronger focus on **privacy, data localisation for critical data, content moderation,** and surveillance on cyber bullying are all on the cards. Further, the government may also be looking to see how anonymised data is democratised to create a more level-playing field for startups and new ventures."

Additionally, the **Digital India Act** will look to bring some basic guidelines for new technologies such as the **metaverse** and the **blockchain** as there is a general sentiment that the current IT Act is inadequate to monitor crimes happening in these ecosystems. For instance, at present most **crypto-related offences** are registered under the IT Act and other aspects of the **Indian Penal Code** that address financial crimes.

THE PATH AHEAD

The internet is rapidly evolving into **'a highly democratized, decentralized, user-definable, virtual and persistent space where virtual and physical realities converge seamlessly – leading to a hybrid, kaleidoscopic reality'** but it remains a baffling place. This makes the task of managing and regulating this amorphous and ever expanding universe so very arduous for the law makers and therefore extensive consultations with academia, subject, and legal experts must be undertaken. Law making at the best of times is a difficult, collaborative and complex process. And when so much is at stake, steps must be taken to prevent partisan politics and vested interests from entering in a big way in such matters and clouding objective discussion.

Any framework devised by the government risks becoming dated in a matter of a couple of years requiring **frequent revisiting** and **repeated amendments** as has happened in case of **IT Act, 2000.** A harsh piece of legislation opens up the government to severe criticism as happened in the case of the **Personal Data Protection Bill** that had to be taken back after five years in the making. Even amendments and secondary legislations have evoked lot of unpleasantness. So, the government has to tread cautiously. However, unambiguous, well worded, precise provisions, prudence in the drafting process and honest intentions can see it through...

A REPORT BY

RED LAB™
Rediffusion Consumer Lab

rediffusion

MUMBAI (Corporate)
1801 Lotus Corporate Park, Goregaon East, Mumbai - 400063
Ph: +91 22 49311000, +91 22 49312000

KOLKATA
10 Wood Street,
Kankaria Estates,
Elgin, Kolkata - 700016
Ph: +91 33 44066262, +91 33 22871232

CHENNAI
1st Floor, Prakash Building,
14, Deivasigamani Road,
Royapettah, Chennai - 600014
Ph: +91 44 28113426, +91 44 28113427

BANGALORE
Unit. No. 401, 4th Floor,
No. 7 Sophia's Choice, St. Mark's Road
Bangalore - 560001
Ph: +91 7838595676

DELHI
The House of Mogae,
112, Udyog Vihar Phase IV,
Gurgaon - 122015
Ph: +91 0124 2345598