Why India must amend its Information Technology Act in the age of Artificial Intelligence

Dr. Chandrika Subramaniyan
Solicitor and Barrister, The Supreme Court of New South Wales, Australia
lawyer.chandrika@gmail.com

The world of technology is changing rapidly and impacting us in a variety of ways. The three important and inevitable technologies gaining widespread momentum and causing profound transformation in the cyber world are big data analytics, Artificial Intelligence (AI), and Internet of Things (IoT). India is the most cyber-branded country in the world due to its human potential, capabilities, and contributions. India and its people have been steadily migrating to the digital world enjoying several benefits that digital technologies offer. But this digital transformation also enhances the risks and threats that digital applications and internet-related activities present which has potential to escalate further. As the 'complex cybersecurity landscape now faces several new threats' as cautioned by San Murugesan(1), it is important for India (as well as other countries) to satisfactorily address cybersecurity and privacy issues. India needs greater and stronger digital governance, code of ethics, regulations, and laws.

The Indian Information Technology Act 2000 (2) (ITA, also known as IT Act) is nineteen years old with a single amendment in 2008.The IT Act provides a legal framework for electronic governance by giving recognition to electronic records and digital signatures,and defines cybercrimes and prescribes penalties for them. The Act also directed the formation of a Controller of Certifying Authorities to regulate the issuance of digital signatures. The amended IT Act 2008 was created to address issues that the original bill failed to cover and to accommodate further development of IT and related security concerns since the original law was passed.(3)

Since the establishment of IT Act in 2008, the digital landscape had changed vastly for good and for worse. The three new major transformative technologies that is transforming Indian digital landscape are Big data analytics, the Internet of Things and Artificial Intelligence. And, the threat to the digital space increases every second and the modern cyberwarfare aims to sabotage citizens and the business, systems, critical national infrastructure and the government. Therefore, it is necessary to significantly change our perception of and approaches to address new cyber risks and threats, This calls for action at different levels including central and state governments to prioritise budgets and amend laws in comparison to those that focus on national security.

Government has no option other than building a holistic approach to 'cyber policy' and establish 'cyber governance' by introducing newer and stricter laws relating to cyber activities. Ever since the IT Act 2000, commonly known as the Cyber Law, came into existence the Cyberworld has experienced many changes. Some of the provisions of the Act have become redundant and incapable of addressing the currently persisting issues and rapidly evolving changes and threats. This necessitates immediate amendment of the IT Act to satisfactorily deal with the current threats and issues in a constantly changing cyber environment.

BIG DATA ANALYTICS

Big data analytics is one of the recent advances in technologies that support high-velocity data capture, storage, and analysis. Currently, it is an important of research and practice.

Cox and Ellsworth were the first to identify the term "Big Data." They defined big data analytics as a "challenge for computer systems: data sets are generally quite large, taxing the capacities of main memory, local disk, and even remote disk" (4).

Data protection laws

Big Data demands more and better legal protection measures. For instance, to enhance 'data protection,' new sections (data protection laws) need to be included in the IT Act. . The increased Cyber activities of individuals and businesses have increased vastly and spans shopping, banking, logistics, travel, gaming, entertainment and social networking, online reviews and comments among others. This has necessitated and resulted in 'information sharing culture' in which personal information like email address, phone number, address, credit card details, personal interests and activities as well as other important personally identifiable information (PII) which is any data that could potentially identify a specific individual such as biometric **information**, medical **information**, and unique identifiers such as driving license number, passport or Aadhaar card number. This increases the risk of cyber-attacks. It is the responsibility of the government to initiate and employ suitable data protection laws in line with the European Union General Data Protection Regulation (GDPR) and other an international standard to ensure the privacy and protection of its citizens, business and industry.

Privacy rights in the International arena

Privacy is a fundamental human right recognized in the Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR), the UN Convention on Migrant Workers and the UN Convention on Protection of the Child, and in several other international and regional treaties. However, privacy has been directly related to the technologies at the time.

Understanding this, Europe changed the privacy laws which are the most significant change. In May 25, 2018, the European Union's General Data Protection Regulation (GDPR) replaced the 1995 Data Protective Directive (DPD). However, the regulation has limitations. The data regulated by the GDPR is applicable to individuals and does not apply to organizations. In addition, the GDPR does not apply to an organization or instances that does not directly deal with or target people in the European Union.

India and Big Data Analytics

The India's Aadhaar programme introduced in 2009 is the world's largest biometric identity platform. It is an initiative of the Unique Identification Authority of India (UIDAI) to help the government provide services to intended beneficiaries. UIDAI, Census of India, Stock Exchange, the Income Tax Department and few other government agencies are employing Big Data Analytics for various purposes. Besides the government sectors, non-state actors including telecom providers and E-commerce businesses use Big Data Analytics to manage their businesses, for example to profile their customers and their behaviours and buying patterns and to predict customer demands and expectations. How much privacy and confidentiality of individuals has been protected by organisations collecting, processing, and retaining large amounts of personal data have been – and continues to be - questioned and doubted. This has led to cases on privacy policy over important issues such as data ownership, involving public and private partnership organisations.

Despite being promised that Aadhaar covers all security risks, it has encountered several controversies including a case in the Supreme Court of India. Activists challenged potential human rights violations found in the Aadhaar framework.(5)It is appalling to note that the Attorney General argued that' people have no 'right to privacy.' This contradicts the constitutional guarantee, "no person shall be deprived of his life or personal liberty except according to the procedure established by law"(6).

UIDAI openly admits on its website that the Aadhar platform allows "third-party developers to develop Web 2.0 applications. The UIDAI's policy and practice of allowing 'third-party developers who are private agencies', to use and leverage its infrastructure and data, raises questions about the privacy and confidentiality responsivity. However, UIDAI states that "biometric information will not be shared with anyone, nor it will be displayed publicly, except for purposes specified by regulations" is giving some solace .However, the balance between 'privacy and purposes specified' looks ambiguous, which leaves the government with the huge responsibility to develop and adhere to stricter regulations at international standards.

INTERNET OF THINGS

The internet of things (IoT) is an evolving system of interconnected objects, people or systems that process and react to physical and virtual information. It aims to enhance user experience or the performance of devices and systems by way of communication between humans, systems, and devices. The IoT market size in India is expected to grow at a rate of 62% CAGR and reach US$9 billion by 2020.(7)

It is imperative, that the communication between multiple devices, and huge data transfer among users, would result in sharing personal information. This will raise concerns about privacy and data protection issues.

'Machine to Machine' (M2M) environment enables data generation and content creation including machine-generated data. This process raises the question related to IP rights of newly generated content/data. This demand M2M service providers to adhere to strict privacy policies to protect the consumer data generated and collected.

In light of this, the government of India released a draft 'Internet of Things Policy' in 2015, aiming to evolve an IoT ecosystem and development of IoT products suitable to the Indian environment. National Telecom (NT) Cell, the government body responsible for policy and regulatory aspects related to M2M communication, released a 'National Telecom M2M Roadmap in May 2015'.Subsequently, TRAI released its consultation paper titled 'Spectrum, Roaming and QoS related requirements in Machine-to-Machine Communications' in October 2016, followed by its recommendations on this consultation paper on 5 September 2017.

The Justice BN Srikrishna committee submitted its report on the data protection law in July 2018 with the following key recommendations. (8)

Individual Consent: It makes individual consent the centerpiece of data sharing, awards rights to users, imposes obligations on data fiduciaries.

Data Protection Authority: Setting up a Data Protection Authority (DPA), an independent regulatory body responsible for the enforcement and effective implementation of the law, holding responsibility for, monitoring and enforcement, legal affairs, policy and standard-setting and research and awareness, inquiry, grievance handling, and adjudication.

Personal Data: The processing of personal data by both public and private entities in India, where data is being used, shared, disclosed, collected or otherwise processed needs cyber monitoring and cyber codes. It is imperative that the critical that personal data of Indian citizens be processed in centers located within the country only. In addition, personal data collected, used, shared, disclosed or otherwise processed by companies incorporated under Indian law will be covered, irrespective of where it is processed in India. However, the data protection law may empower the Central Government to exempt companies, which process the personal data of foreign nationals and the companies not present in India.

Data Storage: The Bill lays out provisions on data storage, making it mandatory for a copy of personal data to be stored in India.

Appellate Tribunal: The Central Government shall establish an appellate tribunal or grant powers to an existing appellate tribunal to hear and dispose of any appeal against an order of the DPA.

Penalties: Penalties may be imposed for violations of the data protection law. The penalties suggested are a penalty of Rs. 15 crore or 4% of the total worldwide turnover of any data collection/processing entity, for violating provisions. Failure to take prompt action on a data security breach can attract up to Rs. 5 crore or 2% of turnover as a penalty.

The penalties paid by violating entities, in this case, will be deposited to a Data Protection Fund, which will, among other purposes, finance the functioning of the Data Protection Authority.

The Bill lays out obligations for fiduciaries to ensure no harm to the user, with transparency and security safeguards;

For data processors not present in India, the Act will apply to those carrying on business in India or other activities such as the profiling which could cause privacy harms to data principals in India.

Impact on allied laws: The report has also listed the impact of the proposed data protection framework on allied laws, including the Aadhaar Act and the RTI Act, which require or authorise processing for personal data for different objectives.

Exceptions: The state can process data without consent of the user on ground of public welfare, law, and order, emergencies where the individual is incapable of providing consent, employment, and reasonable purpose.

Concerns

Though the draft bill addresses various issues plaguing the data ecosystem in India, it falls short on key principles that are at the core of a robust data protection framework.

The Bill proposes that personal data of individuals can be processed for the exercise of any function of the state. This can be done without the consent of the individual as long as it is to provide a service or benefit to the individual. This runs directly counter to the articulation of informed consent as central to informational privacy in the Puttaswamy judgment, 2017.

One key subject missing from the draft bill is the reform of surveillance laws. There is very little legislative and judicial oversight on surveillance activities carried out in India.

As proposed by the Bill, requiring all businesses to store data within India, without any reform of surveillance governance, can pose even bigger privacy issues in the future.

ARTIFICIAL INTELLIGENCE

Artificial Intelligence and Robotics have emerged as powerful transformative technologies of this era, creating data-driven solutions to solve everyday problems.

“Once considered a remote possibility reserved for science fiction, AI has advanced enough to approach a technological tipping point of generating ground-breaking effects on humanity and is “likely to leave no stratum of society untouched”. (See Lauren Goode, “Google CEO Sundar Pichai compares the impact of AI to electricity and fire” (9).

Therefore, it creates a necessity for the government to consider developing a business ecosystem that can leverage artificial intelligence and robotics with proper ethical measures to avoid harmful impacts.

The European Union 's guidelines (10) to develop ethical applications of artificial intelligence are:

- Human safety and oversight
- Technical robustness and safety
- Privacy and data governance
- Transparency
- Diversity, non-discrimination, and fairness
- Environmental and societal well-being
- Accountability

Indian Government also must focus on the above guidelines to implement laws for ethical use of AI.

Bernhard Debatin, an Ohio University professor and director of the Institute for Applied and Professional Ethics (11), says, a good privacy legislation in the age of AI, should include five components:

1. AI systems must be transparent.
2. An AI must have a "deeply rooted" right to the information it is collecting.
3. Consumers must be able to opt-out of the system.
4. The data collected and the purpose of the AI must be limited by design.
5. Data must be deleted upon consumer request.

CYBER RESILENCE

A more agile approach to cybersecurity To ensure that information assets are properly protected, a more agile approach to cybersecurity is required. As advocated by Hult and Sivanesan, an effective cyber agility is essential for organizations to quickly respond to and contain the devastating effects of cyberattacks (12)

An organization which deals with a wealth of easy-to-access data with limited current cybersecurity solutions needs to focus on security issues to mitigate cyber risks in knowledge management and create cyber agility to control cyber-attacks. Knowledge management involves three stages: acquisition, conversion, and application. Cyber agility is increasing the firm's ability to respond quickly by identifying potential cyber threats, detect and measure the frequency and sophistication in detecting imminent threats, and be proactive to protect information assets.

CONCLUSION

India is in the process of enhancing its capacity and competing in the international arena in the areas of Artificial Intelligence, Internet of Things and Big Data Analytics . Therefore, it cannot ignore the Data Protection regime which needs balance in all spheres of society, industry, and government contribution.

The following serve as guidelines for suggestive amendments to the Information Technology Act, and for a holistic approach to addressing privacy issues.

- Efficient Data Protection Law
- Active Cyber Protection Agency
- National Cyber Crime Intelligence and Task Force
- State-level Cyber Policing System
- Technologically competent cyber system to implement physical and digital safeguards of Cyberworld

REFERENCES

(1) Murugesan, San, "The Cybersecurity Renaissance: Security Threats, Risks, and Safeguards," IEEE ICNL, Jan-Mar 2019,http://ieeecs-madras.managedbiz.com/icnl/19q1/p33-p40.pdf <19Novmeber 2019>

(2) https://www.itlaw.in<24 November 2019>

(3) .https://whatis.techtarget.com/definition/Information-Technology-Amendment-Act-2008-IT-Act-2008<25 November 2019 >

(4) Cox M, Ellsworth D. Managing big data for scientific visualization. ACM Siggraph. 1997;97:21–38. Page 4,< last seen on 13/11/2019>

(5) Justice K. S. Puttaswamy (Retd) Vs Union of India. , https://indiankanoon.org/doc/127517806/).< last seen on 13/11/2019>

(6) Article 21 of the Constitution of India ,< last seen on 13/11/2019>

(7) https://www.ey.com/Publication/vwLUAssets/EY_-_Future_of_IoT/$FILE/EY-future-of-lot.pdf).< last seen on 13/11/2019>

(8) https://www.drishtiias.com/daily-updates/daily-news-analysis/justice-bn-srikrishna-committee-submits-data-protection-report.< last seen on 13/11/2019>

(9) https://www.theverge.com/2018/1/19/16911354/google-ceo-sundar-pichai-ai-artificial-intelligence-fire-electricity-jobs-cancer. < last seen on 13/11/2019>

(10) https://www.theverge.com/2019/4/8/18300149/eu-artificial-intelligence-ai-ethical-guidelines-recommendations#:~:targetText=The%20European%20Union%20today%20published,help%20us%20control%20murderous%20robots. < last seen on 13/11/2019>

(11) https://www.forbes.com/sites/insights-intelai/2019/03/27/rethinking-privacy-for-the-ai-era/#59628d817f0a< last seen on 13/11/2019>

(12) Hult F, Sivanesan G. What good cyber resilience looks like. J Bus Contin Emerg Plan. 2014;7(2):112–25

About the author

Dr. Chandrika Subramanian is a well-known solicitor and mediator in the legal community. Her experience in IT has made her a qualified Microsoft professional. She is an Advisory Member of Justice Department NSW, Cumberland Council and Syd West Multicultural Services. She is also a Fellow of Asian Institute of Disputer Resolution. She is the first female chairperson to head Syd West Multicultural Services. Today she has three successfully established businesses in Australia.

She has been teaching at tertiary level, media, leadership and law since 1988 in India at Madras University, Madurai University and Oriental Institute Marina Campus , and Colombo University, Nawala University and Kelaniya University in Sri Lanka and in Western Sydney University and Federation University in Australia since 2000.

Chandrika has been a regular writer and presenter of radio programmes on community education. Her media and leadership workshops are popular in India, Sri Lanka and Australia. She has written 30 books on topics such as Law, Women, Media, Computers and Hinduism in Tamil and English. Her book on ‘Women and Media’ had received the Tamilnadu Government’s literary award in 1988 and recently in 2018, amilnadu Government honoured her with the title ‘Overseas Tamil Scholar’. Her book on ‘Cyber Laws and Cyber Crimes’ received the APJ Abdul Kalam Science and Technology Award from SRM University.

Her other awards in Australia include: Premier’s Harmony Medal Winner 2019 - NSW State Government; Citizen of the Year 2019 - Cumberland Council; Women of the West 2012 - University of Western Sydney; Highly commended Award 2011 – Women Lawyers Association; Nominee Justice Medal 2009 - Justice Foundation

Information Technology Act, 2000 – List of offences

65	Tampering with computer source documents
66	Hacking with computer system
66B	Receiving stolen computer or communication device
66C	Using password of another person
66D	Cheating using computer resource
66E	Publishing private images of others
66F	Acts of cyberterrorism
67	Publishing information which is obscene in electronic form.
67A	Publishing images containing sexual acts
67B	Publishing child porn or predating children online
67C	Failure to maintain records
68	Failure/refusal to comply with orders
69	Failure/refusal to decrypt data
70	Securing access or attempting to secure access to a protected system
71	Misrepresentation

Source: https://en.wikipedia.org/wiki/Information_Technology_Act,_2000

The Information Technology Act, 2000 (also known as ITA-2000, or the IT Act) is an Act of the Indian Parliament (No 21 of 2000) notified on 17 October 2000. It is the primary law in India dealing with cybercrime and electronic commerce. It is based on the UNCITRAL Model Law on International Commercial Arbitration recommended by the General Assembly of United Nations by a resolution dated 30 January 1997