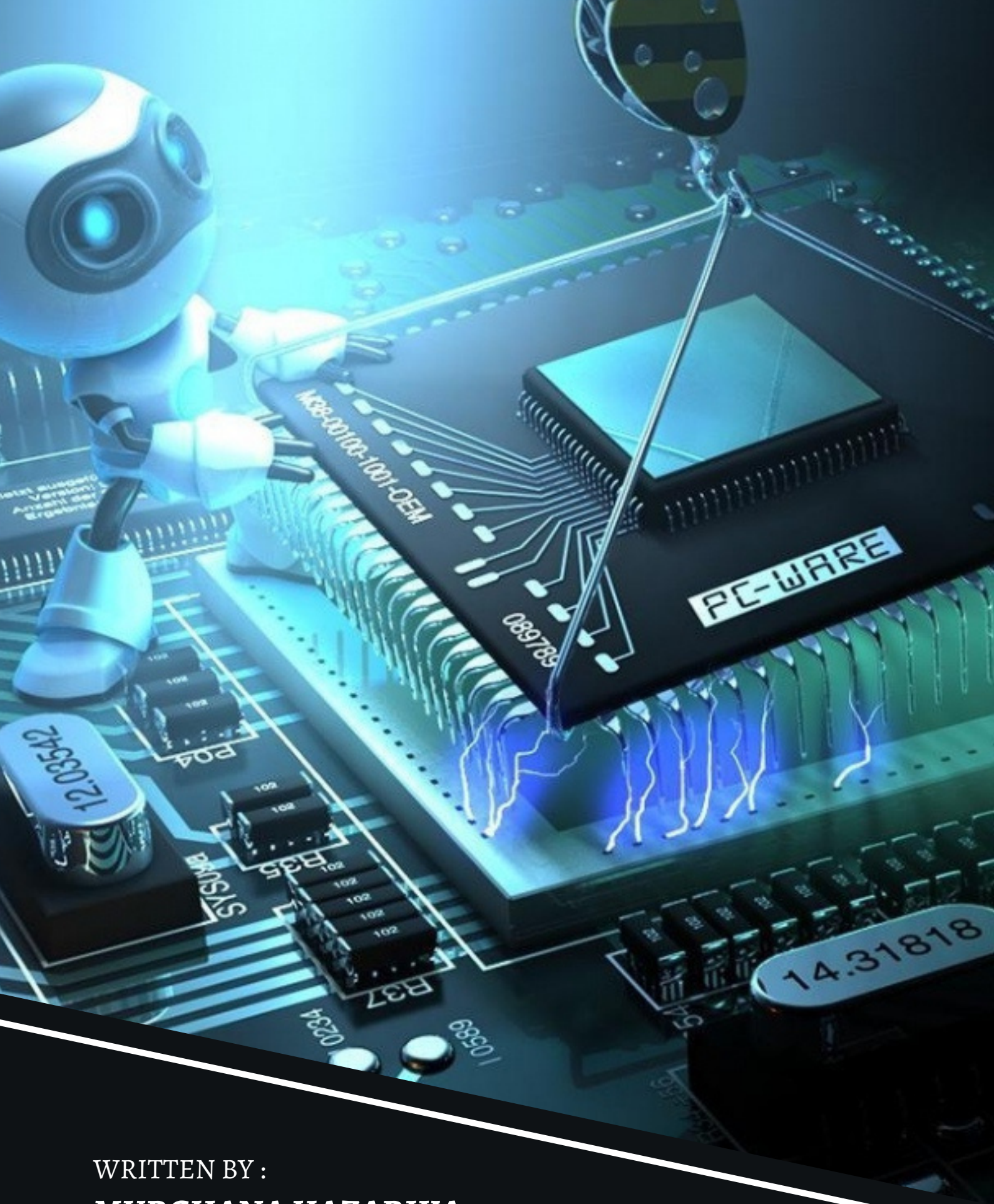
OVERHAUL OF THE INFORMATION TECHNOLOGY ACT OF 2000,

Existing potential for amendments, additions, and recommendations.

Nov 2021



WRITTEN BY :

MURCHANA HAZARIKA

POLICY RESEARCH INTERN - NITI TANTRA,

murchana.hazarika070@gmail.com

INTRODUCTION

The I.T. Act establishes a legal foundation for electronic governance by recognizing electronic documents and digital signatures, as well as defining and punishing cybercrime. The Act also mandated the creation of a Controller of Certifying Authorities to oversee digital signature issuing. The Act was introduced as legislation around the time when only 55 lakh people, which was 0.5% of the population (Garg, Rohin) in India, were acclimated online through online e-commerce websites, being the single source of concern.

The United Nations Commission on International Trade Legislation created a model law on Internet commerce, which was then endorsed by the General Assembly in a resolution (MEITY) requiring governments to give the model law favorable regard when implementing or modifying similar laws. India implemented the ITA 2000 in accordance with the UNCITRAL model law's requirements.

In the current times, a large number of digital domains such as social media websites, governmental digital records, e-governance, artificial intelligence, machine learning, digital wallet, and payment platforms fall under the realms of the I.T. Act. With broadening spectrums and the rising digital presence of Indian citizens, it has become imperative for a process of overhauling the I.T. Act and its sections in order to effectively tackle newer digital concerns and protect the rights of individuals. There has been tremendous growth in terms of digitalization, and as such, efficient policy assurance and implementation by revamping the I.T. Act have become the need of the hour.

FREEDOM OF SPEECH AND EXPRESSION, ARTICLE 19

The section on sending offensive messages through any communication service offers a blanket and unspecified term on what' menacing' or 'grossly offensive' (s.66A.(a)) would imply without delving into elaborate guidelines about the nature of content that would fall under being 'grossly offensive' and 'menacing.' In turn, it is important to understand that this section of the Act teetered on the edge of breaching fundamental rights on the Freedom of Speech and Expression in Article 19 and hence was offered special reviewing by the Supreme Court to shed light on specified definitions/explanations about the content that would be under the umbrella of causing 'annoyance,' 'inconvenience' (s.66A.(b)) et al.

Upon doing so, the provisions of the Act would acquire further clarity on the nature of communication one should keep in mind over digital/online communication methods so as to not violate the guidelines of the Act, and this can only be carried out upon further explanation of the undesired terms offered by this section of the Act. This section failed to provide legal boundaries between 'spam' messages and messages of highly inappropriate nature targeting personal/professional security and hence was struck down by the Supreme Court in 2015 by a bench of Justices J. Chelameswar, and R.F. Nariman ruled in Shreya Singhal v. Union of India declaring Section 66A unconstitutional for "being violative of Article 19(1)(a) and not saved under Article 19(2)." (Indian Express, 2021)

GENDER-INCLUSIVE REVIEWING

Section 66E delves into the sphere of bodily security and autonomy and goes on to specify through defining the term 'private area' through mentions of 'female breast' (s.66E(c)), displaying undertones of gender-based scrutiny by specifying female breasts and participating in the stigma surrounding body positive and gender supportive/neutral terms and leaving out the cause for safeguarding the interests of all citizens irrespective of their gender. It fails to take into account that the exposure of digital reproductions of any individual's physical part irrespective of their gender (he/she/they) is a violation nonetheless and could review the usage of solely the term female and instead take into account bodily autonomy of all citizens across the gender spectrum, irrespective of their assigned sex at birth, i.e., natal sex. (U.W. Medicine)

CONCERNS OF CENSORSHIP

The Central Government has the authority under Section 69A to "give orders for limiting public access to any information through any computer resource." That means the Government would be able to block any website. No rules have been established, despite the fact that necessity or expediency in terms of specific restricted interests has been specified. According to s.69A(2), those recommendations "must be such as may be imposed." Before any censorship powers are provided to any authority, it must be assured that they are prescribed beforehand (Deol et al.). Any law in India that grants an administrative power unguided discretion to implement censorship is inherently unjustifiable (Venugopal, AIR 1954 Mad 901).

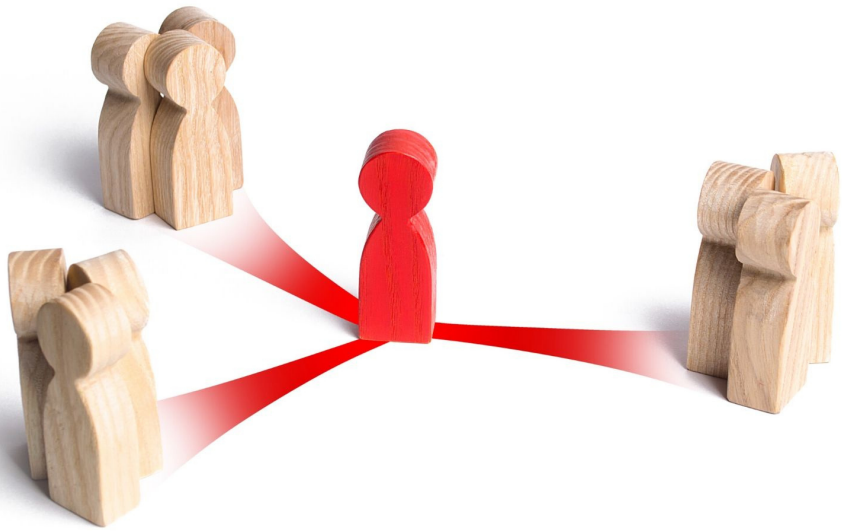
INTERMEDIARY LIABILITY

While the adjustment to the provision on intermediary liability (s.79) is a step in the right direction in that it attempts to hold only the genuine violators of the law accountable, it is still insufficient. This exemption must be broadly written in order to foster innovation and enable corporate and public initiatives for content sharing, including through peer-to-peer technologies. For starters, the demand that content is taken down after receiving "real knowledge" is far too demanding for intermediaries.

As a result of this necessity, the intermediary, rather than the authorized authority, is forced to make choices. Second, that requirement violates natural justice and free speech principles by allowing a communication and news medium to be silenced without providing it or the person communicating via it a fair hearing. Our courts have ruled that a restriction that denies affected people the right to be heard is procedurally unjust (Virendra v. the State of Punjab, AIR 1957 SC 896).

On the other hand, however, according to a recent development, Frances Haugen's latest expose on Facebook about the giant social media fueling hate speech and misinformation on the platform has pushed the Government to probe for algorithmic accountability under Rule 3 of India's recently declared I.T. Rules under the I.T. Act, platforms must exercise "due diligence" when it comes to content that is "grossly hurtful... bigoted, or racially, ethnically offensive... or otherwise unlawful in any manner whatsoever" (The Economic Times).

This highlights Facebook's role as an intermediary in the concern under the intermediary liability function and presents a counter picture from the free speech and content sharing. The Ministry of Electronics and Information Technology (MEITY) intends to enact a stricter intermediary liability framework, which would replace the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (I.T. Rules) and give the Government more control over social media sites. According to some rumors, a new Act may be introduced to address intermediary responsibility directly.



CONCERNS OF IDENTITY THEFT

The I.T. Act does not provide sufficient legal provisions across the Act about safeguarding identity attacks digitally/online and is yet to provide legal respite to prevent the misuse of one's identity when alive and/or post expiry to shun and/or protect the usage of formal documents and governmentally recognized citizenship records through identity theft. With the cause of digitalization furthering itself through e-Aadhar systems et al., it is imperative to provide strict regulations and related punishments in the case of identity theft to prevent loss of personal and financial autonomy that would occur during an instance of identity theft.

Cheating by personation is not defined, and it is unclear whether it refers to cheating as defined by the Indian Penal Code when done through communication devices, or is it a new category of crime. In the latter case, it is unclear whether the court will give those words a narrower meaning, such that only phishing will be punished, or whether other forms of anonymous communication or disputes in virtual worlds (such as Second Life) will be brought under the definition of "personation" and "cheating" (Centre for Internet & Society)

INSUFFICIENT INFORMATION RELATING TO CYBER CRIMES AND CYBER SECURITY

The fundamental goal of the Information Technology Act of 2000 was to ensure that e-commerce was legally recognized in India. As a result, the majority of the rules are focused on developing digital certification systems within the country. The phrase "cybercrime" was not specified in the statute. It only looked at a few examples of computer crimes. As described in Chapter XI of the Act, these acts are:

- Illegal access, the introduction of a virus, denial of service, inflicting harm, and manipulating computer accounts are all covered under Section 43.
- Computer code tampering, destruction, and concealment are all covered under Section 65.
- Acts of hacking that result in unjust loss or harm are covered by Section 66.
- Acts relating to the publication, transmission, or causing the publication of obscene or lascivious material are included under Section 67.

Furthermore, section 76 makes it easier for authorities to seize a disputed computer resource without defining precautions against data loss or tampering, increasing the danger of data breach and misleading implications. Even the criminal penalties established in sections 65 and 66 are confined to tampering with "computer source code" and have shown to be ineffective against AI-driven attacks, as the Pegasus software attack in 2019 demonstrated (Yashaswini).

PERSONAL DATA PROTECTION BILL- A LESSON FROM THE IT ACT?

Currently, India does not have within its ambit a data protection legislation, but with growing markers of digitalization, the I.T. Act has been dealing with digital protection along with the (Indian) Contract Act, 1872. Sections 43A and 67C of the Act, which deals with data protection, require the Act to be updated to reflect modern data protection standards, ultimately pushing the narrative towards the Personal Data Protection Bill, 2019.

In the lack of a strong Data Protection Authority, legal protection of citizens and their presence across the internet has been a cause of concern. Individuals undertake a sizeable chunk of their professional and personal activities through at least a single data/digital transaction in a week, and since a data protection law has the capacity to provide an effective legal remedy to digital woes, it serves as a tool of accountability towards actualizing fundamental rights and provides assurance towards ensuring that data fiduciaries are held accountable through jural means and a holistic data protection legislation.

USING PRE-LEGISLATIVE CONSULTATIVE POLICY OF 2014 AS A MEASURE OF RECOMMENDATION FOR AMENDMENTS TO THE ACT

With the UPA government in India laying the groundwork for the strategy in 2014 when it authorized pre-publication of bills, a Pre-Legislative Consultation Policy is a way of involving and engaging the general public in the development of bills before they are introduced in the Parliament. According to the policy's principles, individual departments and ministries are to make their proposed legislation available to the public along with the provision of elaborate justifications, key elements of the proposed legislation, broad financial implications, and an estimated assessment of the impact of such legislation on the environment, fundamental rights, lives, and livelihoods of the people.

According to the Policy, such information may be retained in the public domain for a minimum of thirty days in order to be proactively shared with the public in the way defined by the Department/Ministry in question. In need of policy overhaul, proper implementation of this form of deliberative democracy on the I.T. Act would act as an effective tool for policy evaluation in the past, as seen from examples from the Kerala Police Act of 2011, the Right to Information Act of 2005 that took into account lived experiences of people and public opinion and as a result lending credibility to the laws enacted through community input as well as ensuring effectiveness since they are more likely to more grounded in reality. Engaging stakeholders and feedback through public opinion would ensure a full consultation duration when amendments are made to the I.T. Act.

CONCLUSION

The inherent flaws within the Information Technology Act of 2000 highlight the ever-growing nature of India's Digital India initiative encompassing citizens across states and linguistic variance. A framework embodying governance methods that ensure the protection of its citizens is of paramount importance, and as such, the overhaul of the Act through additions within the Act as well as introducing legislation supporting the body of the Act remains vital and has been a point of pressure from civil society organizations, data protection and I.T. based public agencies et al. Ensuring the fundamental rights of citizens is a primary measure of all legislative outputs, and as such, the refining of the I.T. Act requires dire, unbiased and crucial legal support through persistent measures of policy evaluation and understanding.

- Garg, Rohin. “After Facebook Exposé: Does India Need to Update Its IT Act?” Internet Freedom Foundation. Internet Freedom Foundation, October 22, 2021. https://internetfreedom.in/facebook-expose-signals-the-need-for-india-to-update-its-social-media-regulations/.

- MEITY. “Preliminary: Ministry of Electronics and Information Technology, Government of India.” Preliminary | Ministry of Electronics and Information Technology, Government of India. Accessed October 26, 2021. https://www.meity.gov.in/content/preliminary.

- Indian Express, 2021. “Explained: The Shreya Singhal Case That Struck down Section 66A of IT Act.” The Indian Express, July 17, 2021. https://indianexpress.com/article/explained/explained-the-shreya-singhal-case-that-struck-down-section-66a-of-it-act-7408366/.

- UW Medicine, “LGBTQ Inclusion: Glossary.” UW Medicine. Accessed October 26, 2021. https://www.uwmedicine.org/provider-resource/lgbtq/lgbtq-inclusion-glossary#:~:text=Assigned%20sex%20at%20birth%20.

- Deol, Taran, Apoorva Mandhani -, Shubhangi Misra -, and Shobhaa De -. “All about Section 69A of It Act under Which Twitter Had Withheld Several Posts & Accounts.” ThePrint, February 2, 2021. https://theprint.in/theprint-essential/all-about-section-69a-of-it-act-under-which-twitter-had-withheld-several-posts-accounts/597367/.

- The Economic Times. “India Seeks Info on Tech, Processes Used by Facebook.” The Economic Times. Accessed October 26, 2021. https://economictimes.indiatimes.com/tech/technology/india-seeks-info-on-tech-processes-used-by-facebook/articleshow/87323177.cms?from=mdr.

- Centre for Internet & Society. “Short Note on It Amendment Act, 2008.” Centre for Internet & Society. Accessed October 26, 2021. https://cis-india.org/internet-governance/publications/it-act/short-note-on-amendment-act-2008.

- Yashaswini. “Update The It Act 2000: India Needs a Reboot!” Internet Freedom Foundation. Internet Freedom Foundation, July 19, 2021. https://internetfreedom.in/update-the-it-act-2000-india-needs-a-reboot/.