Journal of Dharma 48, 3 (July–September 2023), 351–368

ROLE OF ETHICS IN POLITICAL GOVERNANCE VIA SOCIAL MEDIA IN INDIA

Mini Srivastava, Arvind P. Bhanu and Divita Khanna•

Abstract

Social media has given unprecedented power to users in terms of connectedness, collaboration, and community building. Consequently, governments are engaging with citizens on social media on a regular and real-time basis for better connectedness. Notwithstanding the numerous benefits of social media platforms to users and governments, they have also become a hotbed of serious concerns like fake news, hate speech and privacy violation. In this hindsight, the paper highlights how each of these stakeholders contribute to these concerns along with some recent incidents happened in India. It also discusses the existing legal framework and underscores the state's inefficiency in curbing them. The paper advocates instilling strong ethics-based-digital-literacy among users through a model code of conduct. Undoubtedly, this solution is idealistic, time-taking and highly ambitious, yet if it is implemented in letter and spirit, it can become a game changer in making social media safer and more accountable.

Keywords: Digital ethics, Fake news, Hate speech, Privacy violation, Social Media Governance, Social media platforms, Users

---

• **Mini Srivastava** is Research Scholar and Assistant Professor at Amity Law School, Amity University, Noida.

• **Arvind P. Bhanu** is Professor of Law and Research and Additional Director cum Joint Head of Institution at Amity Law School, Amity University, Noida.

• **Divita Khanna** is a Research fellow at Amity Law School, Amity University, Noida.

Acknowledgement: The authors acknowledge Mr. Suvidutt Sundaram, Advocate-on-Record (AOR), Supreme Court of India and Prof. (Dr.) Aditya Tomer, Additional Director and HOI, Amity Law School, Amity University, Noida for their invaluable guidance and insights.

1. Introduction

Since time immemorial, different countries have been choosing different models of political governance depending upon their value systems. Some preferred authoritarian and totalitarian models while others preferred monarchies and oligarchies. Democracies started operating much later in terms of origin. In this regard, English philosopher John Locke in his classic work of political philosophy *Second Treatise of Government* (1689) discusses the nuances of 'Political society'. According to Locke, a political society is one in which people participate voluntarily by a social contract, as opposed to governments formed by monarchy or autocracy. Most of the modern-day governments follow Locke's social contract theory as their basis of origin.

Fast forwarding to modern times, United Nations Economic and Social Commission for Asia and Pacific explains that in governance, there is involvement of both the formal and informal entities in decision-making and execution. Various informal actors that may influence governance are NGOs, research institutions, religious leaders, financial institutions, political parties, military, media, lobbyists, international donors, and multinational corporations, etc.

Further, the modern-day governance in India has also been significantly influenced by social media. Today, various governments at all levels – be it at federal, state, or municipal level, are using social media handles. It is done with two-fold objective: 1) to connect with people more closely to understand their lives better and 2) to serve people more effectively by dissemination and implementation of various policies and programmes at their doorstep. Apart from this, a vast majority of people today are using social media as a preferred medium of communication. As a matter of fact, India is one of the leading locations with over 467 million social media users *(Kemp)*. However, the level of adherence to digital media ethics is low leaving the country vulnerable to large scale online threats.

Hence, it becomes imperative for governments to ensure that the online environment remains safe and secure for its people. However, considering the huge amount of traffic on social media platforms, it is very difficult task for most governments including Indian government. Moreover, the social media platforms, despite making large impact on the country and making huge profits out of it,

have very little focus towards ethic running of platforms. Even if ethics form part of their policies, its implementation at the ground level is not very effective.

In this hindsight, this paper is highlighting the actual and normative online behavior of social media users as well as platforms and governments in India.

2. MAJOR ISSUES IN SOCIAL MEDIA GOVERNANCE

A social media governance scenario typically has three major stakeholders, i.e., users, government, and platforms. Each stakeholder has, either knowingly or unknowingly, used as well as misused the digital environment. Consequently, there has been further disenfranchising of the vulnerable sections of the society, namely women, children, certain races, or cultural groups etc.

Out of total population in India, 33% use social media actively *(Kemp)*. As a large majority of these people are not very conscious about online safety and have low level digital literacy, it makes them extremely vulnerable to various digital threats. Some of the major issues pertaining to social media governance in India which are under the scope of this study are (1) Fake News; (2) Hate Speech and (3) Privacy Violation respectively.

2.1. Fake News

In this digital era of information overload, we are facing a critical issue – proliferation of fake news and false information. Every day, social media users come across several kinds of false information which remain afloat without questioning its source or integrity. It can be in the form of satire, imposter content, false connections, fabricated stories, misrepresentation of facts, manipulated information and memes etc. The purpose of fake news is often to deceive the reader, to influence them or to simply make them question their own opinions. It may also be for political and ideological agendas or for business interests. Sometimes, people engage in it simply for the purpose of their or other people's entertainment. Sometimes, false information is shared deliberately (disinformation) while in many cases, people share such content due to lack of knowledge or clarity on the matter (misinformation). All such information leads to confusion, chaos, disturbances, and disharmony in society.

Governments are as much part of this ecosystem having informational overload, consequently sometimes, the governments

also, directly or indirectly, may end up contributing to the proliferation of fake news. They become the source and spread false information through posts on various social media handles or official statements. Also, they may attempt to censor or control the spread of accurate information by either promoting false information or suppressing true facts thereby restricting people's free speech. Governments may also attempt to manipulate social media algorithms to promote their agenda or to suppress dissenting voices. Even when the Government is not the source, they are failing to enforce strict regulations upon social media platforms to better monitor fake news and restrict its spread.

Social media platforms are primarily dependent on the degree of attention given by the users on the content posted on their website such as likes, shares, and comments. Its truthfulness may not really be required to make content popular. Consequently, these platforms are often enablers or carriers of fake news. It spreads easily on such platforms because anybody may publish anything to a wide audience. Sometimes, social media posts spread conspiracy ideas, which are typically false. Such information intrigues consumers, so social media algorithms generate and suggest it. So, these platforms must monitor and stop bogus news.

Although most of these websites have policies of not becoming platforms for fake news, yet considering the huge amount of content that is shared on social media every second, it is evident that their controlling mechanisms are not sufficiently effective allowing a lot of incorrect information to propagate.

Social media users have also contributed to the spread of fake news either intentionally or simply due to lack of knowledge. They often share information without questioning its source or verifying its authenticity. They may believe in false narratives or conspiracy theories and spread them to large masses. Some users intentionally create and spread false information for entertainment, to gain profit or to spread propaganda or misinformation campaigns. Hence, users must be vigilant of what they believe and share on such platforms.

- **Indian Legal Perspective**

Article 19 of Indian Constitution ensures 'Right to Freedom of Speech

and Expression'. However, sometimes this right is misused to spread fake news and false information. Even though, no specific laws have been codified against fake news, action can be taken if the same can be classified as an offence (hate speech, defamation, etc.) under the various provisions spread across the Indian Penal Code, 1860 (IPC), the Disaster Management Act, 2005 (DMA), the Information Technology Act 2000 etc. to control the spread of Fake News.

Section 54 of DMA states that anybody who provokes panic by disseminating a false alert or warning about a catastrophe, its severity, or its enormity faces imprisonment (up to one year) or a fine.

Section 505(1) IPC states anyone who makes or publishes a statement or spreads a rumour with the intent to terrorize or alarm or instigate the public or classes or communities to commit crimes faces up to three years in prison and/or fine. Also, Section 505(2) IPC stipulates that anybody who makes or publishes any such remarks intending to sow discord, hate, or malice based on caste, race, religion, or any other basis would face the same penalties.

Section 499 & 500, IPC provides that defamation is making or publishing false statements or representations which can cause harm to or tarnish another person's reputation. Its punishment is up to 2 years imprisonment and/or fine.

Section 153, IPC provides that whoever causes provocation malignantly or wantonly with intention to incite riots by doing something illegal, shall be punishable with imprisonment extending up to 6 months (if rioting is not a consequence) or 1 year (if rioting is a consequence) and/or fine.

Section 66A, IT Act provides that whoever knowingly shares false information through electronic mail or messages to inconvenience, insult, etc. another person or tries to deceive, mislead, or cause annoyance to another person, shall be punishable with imprisonment and fine. However, this section was declared unconstitutional in 2015, by the Supreme Court in *Shreya Singhal and Ors. v. Union of India* on the ground of being too broad or vague as well as violative of Article 19 of the Constitution.

- **Position of Fake News in India**

Despite such laws in place, as per National Crime Records Bureau (NCRB) data, India saw massive rise in fake news cases and spread of misinformation from 2019 to 2020 by 214%. *(Madaik)* A study was conducted on spread of misinformation during COVID-19 in 138 countries and India was on top (at 18.07% of total fake news on social media) due to higher internet usage, social media consumption, and lack of digital literacy of Indian citizens.

India witnessed several national controversies due to such rapid spread of misinformation, including several Mob lynching cases

(2017-2018) based on rumors about the victims being child kidnappers or cow smugglers[1]; JNU sedition case (2016) based on false accusations and doctored videos[2]; Attack on Kashmiri students in the aftermath of the Pulwama terror attack (2019)[3]; rumors about manipulation of Electronic Voting Machines during the 2019 Lok Sabha elections[4]; false information regarding Covid-19 remedies having no scientific basis[5]; post-demonetization rumors regarding the new currency notes containing Nano GPS Chip (2017)[6]; Hindu-Muslim Riots (2017) in West Bengal due to unrelated photographs[7]; and the Padmaavat Controversy (2018) which led to riots and violence over a scene which did not exist in the film.[8]

Further, the issue of fake news or false information is handled by the Press Council of India, in relation to news agencies and journalism. Any person who is affected by fake news, may file a grievance with the News Broadcasters Association (NBA), Indian

---

[1] Sakhadeo, Devika. "Mob Lynching in India Based on WhatsApp Rumors Claims Lives of Two Innocent Men." Global Voices 2018, <globalvoices.org/2018/06/15/mob-lynching-in-india-based-on-whatsapp-rumors-claims-lives-of-two-innocent-men> 23 Feb 2023.

[2] The Wire Staff. "JNU Sedition Case: Umar Khalid, Kanhaiya Kumar, Other Accused Appear in Court." The Wire 2021 <thewire.in/law/jnu-sedition-case-umar-khalid-kanhaiya-kumar-delhi-court> 23 Feb 2023

[3] PTI. "Pulwama Attack Fallout: Kashmiri Students Attacked in Maharashtra" The Times of India 2019 <timesofindia.indiatimes.com/india/pulwama-attack-fallout-kashmiri-students-attacked-in-maharashtra/articleshow/68100385.cms> 23 Feb 2023

[4] India Today Web Desk. "Multiple Videos of EVMs Stacked in Cars, Shops Surface on Twitter." India Today 2019 <www.indiatoday.in/elections/lok-sabha-2019/story/evm-manipulation-videos-on-twitter-1530716-2019-05-21> 23 Feb 2023

[5] Bhaduri, Ayshee. "Claims of Black Pepper, Honey, Ginger Curing Covid-19 Is Fake, Tweets PIB." Hindustan Times 2021 <www.hindustantimes.com/india-news/claims-of-black-pepper-honey-ginger-curing-covid-19-is-fake-tweets-pib-101619427423854.html > 23 Feb 2023

[6] Tech Desk. "RBI's New Rs 2000 Notes Do Not Have a Nano-GPS Chip." The Indian Express 2016, indianexpress.com/article/technology/tech-news-technology/nope-rs-2000-note-does-not-have-a-gps-nano-chip-inside-it> 23 Feb 2023

[7] Daniyal, Shoaib. "In-depth: How a Facebook Post Broke the Decades-long Communal Peace of a West Bengal Town." Scroll.in 2017 <scroll.in/article/843692/in-depth-how-a-facebook-post-broke-the-decades-long-communal-peace-of-a-west-bengal-town> 23 Feb 2023

[8] "Padmaavat: Why a Bollywood Epic Has Sparked Fierce Protests." BBC 2018 <www.bbc.com/news/world-asia-india-42048512> 23 Feb 2023

Broadcast Foundation (IBF), and Broadcasting Content Complaint Council (BCCC). These bodies deal with grievances against the content aired by channels and broadcasters, including fake news. Various fact checking websites are also available to Indian citizens such as Boomlive.in, Factrescendo.com, The Quint, Factly.in, India Today, etc. The users can refer to these websites to become better aware of what they share and believe.

Despite having availability of several laws, fact checking mechanisms, and complaint forums etc., the fake news scenario in India has been rapidly worsening; hence an ethical code of conduct for all users is the need of the hour.

2.2. Hate Speech

Hate speech has been a global concern for centuries, even before the emergence of modern media. The United Nations defines Hate Speech as *"any kind of communication in speech, writing or behavior, that attacks or uses pejorative or discriminatory language with reference to a person or a group on the basis of who they are, in other words, based on their religion, ethnicity, nationality, race, color, descent, gender or other identity factor."*

Governments, in general, do not partake in hate speech, but some of its members may engage in it or permit it to occur without much intervention or penalties to the offender practicing hate speech. When Governments do not punish such wrongdoers, it inadvertently creates an environment which fosters animosity and flourishes hate speech. The government has a responsibility to make and implement adequate laws and strategies to tackle hate speech and provide equal respect to all.

Social media platforms' involvement to the issue of hate speech cuts both ways. On one hand, these platforms provide its users a convenient platform to express their views freely. It also granted a voice to marginalized sections which enabled them to enlighten the masses regarding various social and political issues including spreading awareness regarding the adverse impact of hate speech. When the masses gain such knowledge, it puts a great deal of pressure on Governments and others who partake in hate speech to mend their ways. On the other hand, some users abuse this freedom and spread hate either through self-created posts or by sharing someone else's hateful content. Even though social media platforms have policies and technologies in place for the detection and removal of hate speech, it

has been argued that they are ineffective or do not have sufficient control upon the situation.

Users, as individuals and as groups, have exploited the platforms to put across their hateful and discriminatory views. Hate speech is used to reach a like-minded audience, influence the audience, or injure the community or persons targeted. These platforms have been used to harass, intimidate, and stereotype certain communities. Users must report such practices in both real and digital environments. They must not promote such attitudes.

- **Indian Legal Perspective**

The Indian Constitution does not expressly define the term 'Hate Speech', but the courts have interpreted its ambit in various precedents. While the Constitution, under Article 19 provides the Freedom of Speech & Expression, it also acknowledges that such liberty is subject to reasonable restrictions as given under Article 19(2). *(Sundaram & Tomer)*

Indian laws regarding Hate Speech are spread across the Indian Penal Code, 1860 (IPC), Criminal Procedure Code, 1973 (CrPC), Representation of People Act, 1951 etc.

Section 153A IPC provides that anyone who incites hatred between various groups on the basis of their religion, caste, race, place of residence, etc., or who engages in actions that undermine harmony between these groups faces a maximum sentence of three years in prison and/or a fine.

Section 153B IPC provides that anyone who publishes or makes any accusations that are likely to incite hatred, enmity, or ill-will between communities faces up to three years in prison and/or a fine (if the offence is committed at a place of worship the sentence may be increased to five years and/or fine).

Section 295A IPC provides that whoever deliberately or maliciously intends to insult or outrage the religious sentiments of any community or group or Indian citizen to be punished with imprisonment up to 3 years and/or fine.

Section 298 IPC provides that whoever deliberately utters words or makes sounds or gestures to wound religious sentiments or beliefs of any person, to be punished with imprisonment up to 1 year and/or fine.

Section 505 IPC provides punishment for publishing or making statements which incite violence and enmity between different communities.

Section 95, CrPC grants State Governments the power to forfeit and issue warrants against certain publications in any newspaper, book or documents having content which appears to be punishable under Sections 153A, 153B and 295A of the IPC.

Section 125, Representation of People Act provides that whoever in the interest of an election, promotes enmity or hatred among communities based on caste, religion, race, etc., shall be punishable with imprisonment (extending up to 3years) and/or fine.
Section 66A, IT Act (declared unconstitutional) provides that whoever shares content through electronic mail or messages person, which is grossly offensive, shall be punishable with imprisonment and fine.

- **Position of Hate speech in India**

Despite having such laws in place, by 2020, as per the NCRB report, the cases registered under section 153A had increased by almost 500%. (*Jacob*) India witnessed several national controversies due to such rapid increase in Hate speech cases, including, Babri Masjid Demolition Speech (1992) which incited communal riots in several parts of India[9]; Giriraj Singh's Hate Speech (2014) in support of Narendra Modi as BJP's Prime Ministerial candidate where he claimed that those who oppose Narendra Modi should go to Pakistan[10]; Sakshi Maharaj's Hate Speech (2015), where he was accused of blaming the Muslim community for the population growth[11]; Anant Kumar Hegde's Hate Speech (2018), a BJP leader, made a controversial statement about Islam[12]; Jamia Millia Islamia Riots (2019) where protests against the Citizenship Amendment Act (CAA) turned into riots and violence between protesters and the police, including several instances of hate speech and violence[13]; Parvesh Verma openly made

[9] Sharma, Kalpana. "Hate Speech by Media: Will Regulation Really Work?" Newslaundry 2022 <www.newslaundry.com/2022/09/30/hate-speech-by-media-will-regulation-really-work> 23 Feb 2023

[10] IANS. "EC Censures Giriraj Singh for Hate Speech." Deccan Herald 2014 <www.deccanherald.com/content/403340/ec-censures-giriraj-singh-hate.html> 23 Feb 2023

[11] PTI. "Blow for BJP as MP Sakshi Maharaj Booked for Alleged Hate Speech in UP." Deccan Chronicle, 2017 <www.deccanchronicle.com/nation/current-affairs/070117/blow-for-bjp-mp-sakshi-maharaj-booked-for-alleged-hate-speech-in-up.html>23 Feb 2023

[12] Mathew, Liz & Johnson, TA. "Hate Speech: Booked, BJP MP Ananth Hegde Sticks to His Remarks." The Indian Express 2016 <indianexpress.com/article/india/india-news-india/hate-speech-booked-hegde-sticks-to-his-remarks> 23 Feb 2023

[13] Sarfaraz, Kainat. "Hate Speech to Hate Crime at Jamia Millia Islamia anti-CAA Protest." Hindustan Times 2020 <www.hindustantimes.com/india-news/hate-speech-to-hate-crime-at-jamia-millia-islamia-anti-caa-protest/story-awP2l5wJORcST8Ff0yA0qM.html> 23 Feb 2023

offensive statements in reference to the Shaheen Bagh Protest against the CAA (2020)[14]; and Praveen Togadia's controversial statements in the public hurting sentiments of the Muslim community.[15]

In a diverse society like India, spread of hate speech can have serious and widespread consequences bringing a feeling of disharmony between communities, cultural groups, or individuals. Higher control on hate speech and better awareness about ethical social media practices can significantly help in improving the situation.

2.3. Privacy Violation

The Universal Declaration on Human Rights (UDHR) provides Article 12 which states *"No one shall be subjected to arbitrary interference with anyone's privacy, family, home, or correspondence nor to attack upon his honor and reputation. Everyone has the right to protection of the law against such interference or attacks".*

Preserving privacy is crucial for safeguarding fundamental aspects of human dignity, maintaining personal safety, and upholding individual autonomy. This article specifically focuses on Information Privacy as it is related to social media. It pertains to an individual's capacity to autonomously ascertain the circumstances, manner, and objectives surrounding the handling of their personal information by other people. Privacy violations can take place through data mining by third parties without the consent of the users, through malware corruption, through phishing attacks, etc. For instance, in 2019, several Instagram users fell prey to a phishing campaign where users were prompted to log in to a hoax Instagram page as part of a two-factor authentication system. Though, in many cases, the users may consent to such violation due to their own negligence or lack of knowledge.

Governments have also contributed to this issue of privacy violation by opting both unethical and ethical means. Some governments

[14] Kumar, Kunal. "Hate Rant by BJP MP Parvesh Verma, Says Shaheen Bagh Protesters Will Enter Houses, Rape Sisters and Daughters." India Today 2020 <www.indiatoday.in/elections/delhi-assembly-polls-2020/story/bjp-mp-parvesh-verma-shaheen-bagh-clear-protest-delhi-election-1640808-2020-01-28> 23 Feb 2023

[15] TN National Desk. "Praveen Togadia's Aide Makes Hate Speech in Gujarat, Fires Derogatory Slur Against Muslim Women." TimesNow 2022 <www.timesnownews.com/india/praveen-togadias-aide-makes-hate-speech-in-gujarat-fires-derogatory-slur-against-muslim-women-article-90722428> 23 Feb 2023

implement mass surveillance programs, cyberattacks, or warrantless searches that collect and monitor citizens' personal data and communication thereby violating privacy rights of people.

Even when Governments opt ethical means and are not the violators themselves, they can indirectly enable such violation through data breaches at government entities or non-implementation of robust data protection legislation, enabling private firms and other organizations to acquire and utilize personal data in ways that breach privacy.

Social Media Platforms are at the very root of the issue of privacy violation. These platforms often lack transparency about their collection method and use of sensitive user data, leaving most users unaware as to what information has been collected and how it is being used. Some platforms collect and use personal data in ways that violate user privacy, such as selling this information to advertisers or using it for targeted advertising. Some platforms have inadequate security measures in place, due to which cybercriminals access and use sensitive personal information. Also, some platforms have default privacy settings allowing the collection and use of personal data thereby violating user privacy. Hence, it is the responsibility of such platforms to be transparent and accountable in their collection and use of personal data, and to implement strong security measures to protect user privacy.

Users have also majorly contributed to this issue due to their negligent behavior, lack of knowledge and vigilance as well as sometimes due to mal-intentions. Most users freely publish personal information on such platforms and forums, rendering them exposed to privacy violations and cyber-crimes. Users may also give their personal details to other online frauds and phishing assaults. Users typically don't read these sites' terms & conditions and privacy rules, which can lead to their personal data being shared or misused. Even if the site recommends a strong password, users might make themselves exposed by not using one. Some people transmit harmful software or links and spams carrying a virus to access sensitive personal information of other users, while others fail to take precautions and fall prey to such malware, giving it access to their device and helping privacy violations. Users must safeguard their sensitive data. They must maintain their privacy and access all pertinent information. For example, the terms and conditions of Facebook provide that whatever original content users upload on their profile shall become the

property of Facebook and they can use the same however they like. They may even gain profit from it to which no user shall be entitled. Many other platforms use the same method to collect and sell private information of users for profit. Recently, WhatsApp tried the same approach and failed.

- **Indian Legal Perspective**

The "Right to Privacy" is safeguarded under Article 21 (Right to life and Personal Liberty) of Part III of the Indian Constitution. The Supreme Court ruled in the historic *Puttaswamy v. Union of India* case (2017) that the right to privacy is guaranteed by the Indian Constitution.

The Information Technology Act, 2000 has some provisions which have some indirect bearing with privacy.

Section 43A of the Act, provides that a corporate entity, that handles or possesses sensitive personal data, is required to pay damages to any individual who suffers unjustified loss or gain as a result of the corporate entity's failure to put in place appropriate security measures to protect the data.

Section 72A of the Act provides that intentional revelation of information obtained via a valid contract that results in or is likely to result in unjust injury to the party in question is punishable by up to three years in jail and/or a fine of up to five lakhs.

Section 65 of the Act provides that there is a three-year maximum sentence for imprisonment and a two-year maximum fine for willfully hiding, destroying, or changing any computer source code that must be kept secret under current law.

Section 66D of the Act provides the penalty for personation using a computer source to cheat another person i.e., imprisonment (extending up to 3 years) and a fine (extending up to 1 lakh)

Section 69 of the Act is an exception to privacy violation and provides that the Government, if it deems necessary for public interest, may intercept, decrypt, or monitor any information in any computer source, even sensitive personal information.

Today, there are 850 million Indian users on the internet and India is considered *"the world's largest digitally connected democracy" (Ministry of Electronics and Information Technology)* having multiple intermediaries (OTT platforms, social media, e-commerce, etc.) and newer, more complex forms of digital threats (cyberstalking, catfishing, proliferation of hate speech, fake news etc.) have emerged. Hence, to combat this issue and improve digital security, the MEITY has proposed the 'Digital India Act, 2023' which will replace the IT

Act, 2000 and enforce new regulations which are fit to combat the current cyberspace issues.

Another important development is that India has recently enacted Digital Personal Data Protection Act 2023 in August 2023 (enforcement in January 2024). Its primary purpose is to ensure the protection and confidentiality of individuals' digital personal information. It places emphasis on safeguarding the rights of individuals regarding their data and ensuring the lawful handling of such information. Its key principles are consent, purpose limitation, data minimization, accuracy, security, and accountability. Individuals have rights *qua* access, rectification, deletion, redress of grievances, and nominating a representative. Penalties for noncompliance vary from Rs. 10,000 to Rs. 250 crores, depending on the type and severity of the violation.

However, there is a flip side to it. One of the exemptions has been provided regarding data processing by the state on the grounds of national security. It may allow the state to withhold far more data than what is necessary thereby impacting the right to privacy of individuals.

Overall, the new legislation is hoped to bring a new age of data security that balances the needs of people and companies in the digital world *(Srivastava)*.

- **Position of data privacy breaches in India**

Despite having such laws in place, there has been a steep rise in privacy violation and data breach cases in India. In 2020, over 700 cases were filed under the Indian IT Act for privacy violation *(Times of India)* and the number has just been increasing. However, the current digital scenario is beyond the scope of the IT Act, 2000 and its amendments or rules as it was mainly created for the regulation of e-commerce in the 2000s. Thus, it is not well equipped to deal with the current challenges in the digital environment.

India has witnessed various controversies due to data breaches, privacy violations and inadequate privacy laws, including the Aadhaar Data Leak (2018) where Aadhaar data of the citizens who enrolled in India's National Biometric Scheme was leaked online[16];

[16] Sapkale, Yogesh. "Aadhaar Data Breach Largest in the World, Says WEF's Global Risk Report and Avast." MONEYLIFE 2019 <www.moneylife.in/article/aadhaar-

Pegasus Spyware Controversy (2020), it was reported that the Indian government was using spyware to monitor the phones of activists, lawyers, and journalists;[17] Ola Data Leak (2019) where the personal data of millions of users of the ride-hailing app Ola had been leaked online[18]; Jio Data Leak (2017) where the personal data of millions of users of the mobile network operator Reliance Jio had been leaked online[19]; Zoom security concerns (2020) about the security of the video conferencing app Zoom, which had several vulnerabilities that could allow hackers to access users' webcams and microphones[20]; Covid-19 test results of several Indian citizens were made public (2021), Domino's India Data Breach (2021) where the data of millions of customers was auctioned on the dark web; and Air India Cyber Breach (2021) where the data of millions of passengers was compromised and leaked.[21]

3. Model Code of Conduct for All Stakeholders in the Digital Environment

It is clear from the above discussion that neither social media users nor government nor social media platforms are keeping ethics at the center while dealing with social media respectively. Consequently, the paper proposes a model code of conduct for these stakeholders so that

---

data-breach-largest-in-the-world-says-wefs-global-risk-report-and-avast/56384.html> 24 Feb 2023

[17] "India: Spyware Use Violates Supreme Court Privacy Ruling." Human Rights Watch 2021 <www.hrw.org/news/2021/08/26/india-spyware-use-violates-supreme-court-privacy-ruling> 24 Feb 2023

[18] Dhapola, Shruti. "OlaCabs Hacked, Credit Cards Accessed; Company Says There Was No Data Breach." The Indian Express 2015 <indianexpress.com/article/technology/social/group-claims-to-hack-olacabs-company-says-no-security-lapse> 24 Feb 2023

[19] Tech Desk. "Reliance Jio Data Breach: Here's Why It Is a Big Deal, What It Means for Users and More." The Indian Express 2017 <indianexpress.com/article/technology/tech-news-technology/reliance-jio-data-breached-120-million-users-why-it-matters-what-it-means-for-you-and-everything-to-know-4743592> 24 Feb 2023

[20] Spadafora, Anthony. "Zoom Security Issues: What's Gone Wrong and What's Been Fixed." tom's guide 2022 <www.tomsguide.com/news/zoom-security-privacy-woes> 24 Feb 2023

[21] "Biggest Cyber Breaches in India." Policybazaar 2023 <www.policybazaar.com/corporate-insurance/articles/biggest-cyber-breaches-in-india> 24 Feb 2023

social media becomes more secure platform for expressing oneself.

Government

- The government should respect people's privacy when using social media platforms and not use personal data improperly or for purposes other than those permitted by law.
- It should be open and honest about how it uses these platforms, including the goal, extent, and possible effects of its activities.
- It should refrain from misinformation or disinformation efforts.
- It should not use social media platforms for propaganda or to sway public opinion.
- It should have reliable methods and procedures for fact-checking and take appropriate action against those who disseminate incorrect information or fake news.
- It should uphold the values of free speech and refrain from censoring content or using social media to silence opposing viewpoints, unless required by law.
- When utilizing social media platforms, it should try to be unbiased and fair, and it should not discriminate against any people or groups based on their colour, ethnicity, religion, or other characteristics.
- It ought to be responsible for how it uses social media and ought to allow people a way to voice complaints or concerns about what it does.

Social Media Platforms

- Social media sites should put user privacy first and do everything they can to keep user data safe from people who shouldn't have access to it or who might use it in the wrong way.
- They should be clear about how they gather and use data, as well as their methods and how they moderate material.
- They should try to be fair and unbiased when they moderate content, and they should not favour or dislike people or groups because of their race, ethnicity, religion, or anything else.
- They should be responsible for the content they host, and they should quickly remove any content that is illegal, harmful, or false within a reasonable amount of time.
- They should support the right to free speech and let people say what they think and believe if it does not break the law or community values.

- They should make sure that all users can access their content, even those with disabilities or limited technology.
- They should be responsible for their actions and decisions and give people ways to voice concerns or complaints about what they're doing.

Users

- Treat others with respect and dignity, regardless of their opinions, beliefs, or backgrounds.
- Avoid bullying, harassment, or hate speech.
- Be mindful of the information you share online, especially sensitive information such as personal details or private conversations.
- Before sharing information or news, verify its accuracy and authenticity to avoid spreading misinformation or fake news.
- Do not misrepresent yourself or your intentions online. Be clear about your affiliations, motives, and the sources of your content.
- Read and follow the terms of service and community guidelines of social media platforms to avoid violating their policies or rules.
- Before posting photos or videos of others, seek their consent and respect their right to privacy.
- Use social media to engage in productive conversations and share diverse perspectives. Avoid attacking or shaming others for their opinions.
- If you encounter any unethical behavior on social media, report it to the appropriate authorities or platforms.

4. Conclusion

India is among the largest consumers of data on social media. Unfortunately, its digital environment continues to remain quite unsafe. In this regard, the paper advocates two solutions – (1) model code of conduct for social media usage; and (2) widespread adoption and promotion of digital literacy campaigns by all stakeholders – users, governments, and social media platforms. It can never be overstressed that ethics must lie at the center of any governance system, and social media governance is no exception to it. A lot of problems can be solved if first and foremost, users learn to use social media responsibly and consciously post/share only lawful content. Thereafter, the illegal and harmful content should habitually be flagged by users. Also, with the help of AI and other checking

mechanisms, harmful content should be flagged and dealt appropriately by moderators at social media platforms. Further, the government should use its agencies and mechanisms to remove harmful content and punish the wrong doers appropriately within its jurisdiction. To sum up, it is ultimately the Ethics which have the potential to be the game changer in political governance via social media in India.

References

Explained Desk. "SC Directions on Hate Speech: How Courts Have Read IPC Sec 295A, Other Provisions." *The Indian Express* 2022 <indianexpress.com/article/explained-law/hate-speech-ipc-sec-295a-supreme-court-8224954.> (10 Mar 2023).

Jacob, Nidhi. "Data Check: In Seven Years, India Has Seen a 500% Rise in Cases Filed Under Its Hate-speech Law." Scroll.in 2022 <scroll.in/article/1026701/data-check-in-seven-years-india-saw-a-500-rise-in-cases-filed-under-its-hate-speech-related-law.> (10 Mar 2023).

Justice K. S. Puttaswamy & Anr. vs Union Of India & Ors, 2017, AIR 2017 SC 4161 (Supreme Court of India, 2017).

Kemp, Simon. "DIGITAL 2023: INDIA" DATAREPORTAL 2023 <https://datareportal.com/reports/digital-2023-india#:~:text=India%20was%20home%20to%20467.0,percent%20of%20the%20total%20population.> 10 March 2023.

Madaik, Devyani. "India Saw 214% Rise in Fake News, Rumour Cases in 2020: Report." The Logical Indian 2021 <thelogicalindian.com/trending/india-saw-214-rise-in-fake-news-rumour-cases-in-2020-report-30723.> 10 March 2023.

Maniyar, Zahid. "An Indian Law on Hate Speech: The Contradictions and Lack of Conversation" CJP 2022 <cjp.org.in/an-indian-law-on-hate-speech-the-contradictions-and-lack-of-conversation.> 8 March 2023.

Ministry of Electronics and Information Technology "Dialogues on the Proposed Digital India Act on 9th March in Bengaluru, Karnataka." MEITY, Government of India 2023 <Www.meity.gov.in, www.meity.gov.in/content/digital-india-act-2023.> 11 March 2023.

Olan, Femi, et al. "Fake News on Social Media: The Impact on Society -Information Systems Frontiers." *SpringerLink*, 19 January 2022

"Privacy and Data Protection Laws in India" Khurana and Khurana

2022 <www.khuranaandkhurana.com/2022/11/09/privacy-and-data-protection-laws-in-india> 10 March 2023.

PTI. "Over 700 Cases Registered Under IT Act in 2020 for Privacy Violation" The Times of India 2021 <timesofindia.indiatimes.com/business/india-business/over-700-cases-registered-under-it-act-in-2020-for-privacy-violation/articleshow/88207723.cms.> 10 March 2023.

Sharma, Tanya and Agrawal, Dhairya. "Law Regarding Fake News in India."Lexlife India 2020, <lexlife68840978.wordpress.com/2020/05/28/law-regarding-fake-news-in-india.> 10 Mar 2023.

Shreya Singhal and Ors. v. Union of India, 2015, AIR 2015 SC 1523 (Supreme Court of India, 2015).

Srivastava, Sameer. "India's Digital Personal Data Protection Act, 2023 (DPDPA): Key Takeaways," 2023.

Sundaram, Suvidutt and Tomer, Aditya. "RELIGIOUS HATE SPEECH vs PEACEFUL CO-EXISTENCE." *Journal of Dharma*, 47.4, 31 Dec. 2022, pp. 473–492.

United Nations. "Universal Declaration of Human Rights" United Nations 2012 <https://www.un.org/en/about-us/universal-declaration-of-human-rights#:~:text=Article%2012,against%20such%20interference%20or%20attacks.> 10 Mar 2023.

United Nations. "What Is Hate Speech?" United Nations 2022 <www.un.org/en/hate-speech/understanding-hate-speech/what-is-hate-speech> 10 Mar 2023.