International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Content Regulation in the Light of Constitution and Data Privacy

Aleena Henry[1], Sona Maria Anto[2]

[1,2]Bharata Mata School of Legal Studies

ABSTRACT

Justice Louis D. Brandeis had said, "The greatest dangers to liberty lurk in insidious encroachments by men of zeal, well-meaning but without understanding."[1] These words depict the challenges of balancing content regulation and data privacy within any legal framework. In India, the landscape of content regulation in the context of the Constitution and data privacy is a multifaceted issue that straddles the line between individual freedoms and state control. Indian Constitution, guarantees the right to freedom of speech and expression through Article 19(1)(a), which includes the right to access and circulate diverse content. Whereas, Article 19(2), circumscribed this right which permits the imposition of reasonable restrictions in the interest of sovereignty, public order, national security, and other concerns. This constitutional framework paves the baseline for content regulation policies, primarily governed and regulated by the Information Technology Act, 2000, and its amendments. They aim to maintain public order and protect national security by regulating, blocking, or removing digital content that is deemed harmful. Nevertheless, these regulatory measures often spark debates regarding overreach and censorship. The state's broad scope of regulatory authority often leads fingers to the arbitrary restriction of free expression and the suppression of dissenting voices. This tension is further intensified, particularly with the introduction of certain other Bills creating cracks within. Through an extensive analysis over the constitutional law, regulatory frameworks, and privacy concerns, this paper maps the current landscape of content regulation and data privacy in India, focusing on the nature and scale of digital media use. It delves into the historical background shaping regulatory frameworks, explores the challenges, and reviews recent reforms and legislation. By examining these issues through an international lens, diverse approaches and efforts to harmonize regulatory measures with the protection of personal liberties.

Keywords: Constitution, Content Regulation, Data Privacy, Information Technology Act, Censorship

INTRODUCTION:

The word "privacy" is derived from the Latin words '*privatus'* and '*privo'*, which mean "set apart from what is public" and "deprivation". In modern usage, privacy is the right to be let alone, or freedom from interference or any intrusion[2]. Data privacy is inferred as an individual's ability to control how personal information like name, location, or behaviour is shared with others. As there has been a massive expansion in internet usage, so has the need for strong privacy measures have emerged, especially when these platforms fail to safeguard it properly. Data privacy is crucial for building trust, as it is often misused for

[1] Olmstead v. U.S., 277 U.S. 438 (1928) (dissenting)
[2] International Association of Privacy Professionals, What is Privacy, IAPP (last visited Sept. 20, 2024), https://iapp.org/about/what-is-privacy/

fraud and harassment. Over the years, the concept of privacy has expanded significantly. Initially concerned with individuals' physical and personal spaces, privacy now encompasses sensitive personal data such as medical records and biometric information. Beyond the legal and financial impacts, privacy is often considered an intrinsic human right, fundamental to freedom and personal expression in a democratic society. Privacy as a human right has been cherished for centuries but has not yet been accomplished. Even though most countries have recognised privacy as a fundamental right, it still lacks sufficient catalyst to protect them. In India, the right to privacy has been recognised through the ambit of Articles 19 and 21. By virtue of Article 21, the right to privacy is considered a personal liberty. The inclusion is the result of a series of significant judicial precedents.

Nevertheless, digital media has become an essential part of human lives creating an immediate risk to privacy. There are about 5.17 billion active digital media users, which covers 63.7 % of the total world population. According to Forbes, Active Social Media Penetration in India is 33.4%. In the current landscape of digital media use competent legislations are crucial for the safeguard of users.

HISTORY

Privacy, even though a generally accepted right from the 19th - 20th centuries, its existence was marked long before that. Privacy is rooted in ancient societies and has a long history. There is Biblica's reference to the violation of privacy where intrusion into someone's private sphere follows shame and anger. Adam and Eve covered their bodies with leaves to safeguard their privacy[3]. In the legal landscape, the Code of Hammurabi and Roman Law contained a paragraph against the intrusion of someone's home[4]. Traditionally, the idea of privacy comes from the distinction made between “public” and “private”.[5] This distinction arises from the natural urge of an individual to make a distinction between himself/herself and the external world.[6] The boundaries between public and private life change from time to time and vary from society to society as it mainly depends upon what people consider as private.[7]

In the ancient periods, an individual's private life was heavily influenced by the state which limited their autonomy and freedom. Plato in his work “Laws”, illustrated that the life of an individual was determined by the state and its goals which resulted in no place for individual freedom and autonomy. The book also states that an individual's life is intent on public interests. Whereas, in the Medieval Age, Privacy was not valued much and individuals were part of a community where their private life was constantly monitored by others. Real privacy began to emerge with the rise of cities. In the 19th century, economic and social changes changed the way people lived which also affected privacy, separating physical and mental privacy. Urbanization led to an increase in population and people living in crowded cities thus reducing physical privacy. But people gained a new sense of privacy which was free from any village scrutiny. The

[3] Konvitz, M. R.: Privacy and the Law: a Philosophical Prelude. Law and Contemporary Problems Vol 31, No. 2. (1966) p. 272.
[4] Solove, D. J.: Nothing to Hide: the False Tradeoff between Privacy and Security. New Haven & London: Yale University Press, 2011. p. 4.
[5] Szabó M. D.: Kísérlet a privacy fogalmának meghatározására a magyar jogrendszer fogalmaival. Információs Társadalom 2, 2005. p. 45.
[6] Konvitz 1966. p. 274.
[7] American law professor Daniel Solove made an illustrative example to present the on-going change regarding what people consider private: even the aspects of life that nowadays are commonly considered as private (the family, the body and the home, etc.) had been through considerable changes as initially they were far from being private. For example, marriage was initially considered to be a contract, while nowadays it is one of the most intimate decisions made by the individual. See more: Solove, D. J.:

appearance of tabloids further gave rise to spreading gossip which impacted privacy. Samuel D. Warren and Louis D. Brandeis recognised these privacy threats in their article "The Right to Privacy" in 1890.

INTERNATIONAL PERSPECTIVE ON PRIVACY

Legal regulations: Beginning in the late 20th century, several international documents recognized the right to privacy as a fundamental right, which was then considered and included in the national laws of different countries. These documents vaguely address privacy, instead, court decisions interpretations and clarifications of what privacy is and what aspects of life are private cleared the hue. The rise of computers in the 1970s raised questions about whether the right to privacy could protect private life and the technological change led to the creation of a new right: the right to data protection.

Various International human rights conventions mention the right to privacy at both global and regional levels. *Article 12* of the *Universal Declaration of Human Rights (1948)*, *Article 17* of the *International Covenant on Civil and Political Rights (1966)*, *Article 8* of the *European Convention on Human Rights (1950)*, and *Article 7* of the *Charter of Fundamental Rights of the European Union (2000)* affirms that privacy is a fundamental human right and that everyone has the right to have a private life, family life, home and communications respected and protected from unlawful interference. However, the articles are quite brief and do not provide detailed definitions. Whereas, the *European Convention of Human Rights* (hereinafter referred to as ECHR) states in *Article 8* that:

"Right to respect for private and family life

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

Numerous countries in Europe, Asia, and America have privacy laws. There are common features in how different countries protect privacy and individual rights. Key principles include limiting personal data collection to specific purposes, using data only for those purposes, allowing individuals to understand the rules about their data, and identifying who is responsible for following privacy laws. Countries differ in their approaches based on the scope of their laws, what they prioritize in protection, exceptions in law, and their enforcement methods. The common principles include:

1. *Notice*: Informing individuals about data collection.
2. *Choice and Consent*: Getting permission before collecting personal information.
3. *Collection Limitation*: Only collecting necessary information which is needed.
4. *Use Limitation*: Using data only for its intended purpose.
5. *Access and Correction*: Allowing individuals to access and correct/update their information.
6. *Security:* Protecting data from loss or theft.
7. *Disclosure to Third Parties*: Requiring consent to share personal information with others.
8. *Openness:* Being transparent about data collection and use.
9. *Accountability:* Holding data controllers responsible for data safety and use.
10. *Preventing Harm:* Protecting individuals whose data is stored.

These principles are recommended for future privacy frameworks as well

The clear definition of privacy is still unclear. It has been the reason for many controversies regarding privacy in different countries.

Legislation in other countries

GERMANY

It is one of the countries with strict privacy laws. Recently these laws have made it difficult for companies like Facebook and Google, which rely on internet freedom.

UNITED STATES

The US Constitution does not directly mention the right to privacy, the Supreme Court has interpreted various amendments to support it. In 1974, the Privacy Act was passed to protect citizens from federal agencies misusing their records.

CANADA

The privacy law in Canada started in 1977 with the Canadian Human Rights Act for data protection. In 1983, it was updated to control how the Government accesses and shares personal information. The law was last changed in 2012 when the Canadian Government stated the Right to personal privacy as a "tort of intrusion upon seclusion".

SWEDEN

Sweden was one of the first countries to give citizens a personal identification number to interact with the government. It also has detailed online privacy laws, starting with the Data Act of 1973 which protected personal data on computers. The Swedish Constitution also includes the right to protect personal data.

EUROPEAN UNION

The Data Protection Directive by the European Union, created in 1995, controls how personal data is handled in the EU. Article 8 of the European Convention on Human Rights gives people the right to privacy, with some restrictions.[7]

AUSTRALIA

Australia has its own 'Privacy Act' created in 1988. It controls how the personal information of the individuals is handled.

JAPAN

In 2015, Japan started a citizen identification that combined tax info, social security, and disaster relief. Each citizen and foreign resident received a 12-digit 'My Number' to improve administration and make social welfare benefits more efficient while reducing tax evasion and fraud. It was voluntary in 2018. Japanese law doesn't directly state a right to privacy, but Article 13 of the Constitution is the right to "life, liberty, and the pursuit of happiness" and the right for people to be "respected for individuals".

Brazil

Brazil's Constitution states , "The intimacy, private life, honor and image of the people are inviolable, with assured right to indenization by material or moral damage resulting from its violation."

A BRIEF HISTORY OF RIGHT TO PRIVACY

The Right to Privacy was not directly incorporated in the Indian constitution by its framers and also does not find a place as a fundamental right as such in part III of the constitution. Despite that, the judiciary has taken significant steps to interpret privacy as a fundamental right from the very start of independence. It was however in 1954, the question of privacy was put forward to the Supreme Court seeking an answer, In the *MP Sharma vs Satish Chandra*[8] case, the Supreme Court decided in favour of the practice of search and seizure when contrasted with privacy. In 1962, while deciding the Kharak Singh vs State of UP [9](AIR

[8] AIR 1295, 1964 SCR (1) 332
[9] AIR 1963 SC1295

1963 SC1295), the Court examined the power of police surveillance with respect to history sheeters and it ruled in favour of the police, saying that the right of privacy is not a guaranteed right under the Constitution. This marked the opening of the tussle between privacy and fundamental rights. 1975, for India, is marked as a Breakthrough year in the light of the right to privacy. In *Gobind v. State of Madhya Pradesh & ANR*[10], the Supreme Court of India introduced the compelling state interest test from American jurisprudence, signaling a key moment in the evolution of privacy rights. The Court acknowledged that while individuals have a right to privacy, this right is not absolute and may yield to greater state interests, provided those interests are convincing and necessary. This marked the beginning of a legal framework where privacy was recognized but balanced against broader public concerns.

In the 1997 *People's Union for Civil Liberties (PUCL) v. Union of India* [11]case, also known as the "telephone tapping case," the Supreme Court made a landmark ruling. It held that individuals have a legitimate privacy interest in the content of their phone conversations, affirming that the right to privacy is extended to communications.

Through a series of rulings, the Indian judiciary gradually strengthened privacy as a fundamental right, while also carving out exceptions where state interests could justify privacy intrusions. The 21st century, however, brought new dimensions to the debate, particularly around the government's Aadhaar program. In 2013, the Supreme Court, responding to these concerns, limited the use of Aadhaar, allowing it only for the Public Distribution System (PDS) and LPG subsidies[12]. However, as Aadhaar became increasingly integrated into India's governance and welfare schemes, the Court amended its earlier order in 2015. Aadhaar's use was extended to programs such as MNREGA, the Pradhan Mantri Jan-Dhan Yojana, and pension and provident fund schemes. Despite these changes, the Court stressed that no individual should be denied access to services for not having Aadhaar. These Supreme Court interventions map a nuanced approach to the landscape of privacy in India.

LEGISLATIONS IN INDIA

Constitution:

In today's civilisation, privacy is widely recognised both in legal terms and in everyday understanding. The right to privacy is a multi-faceted and complex concept. In the Indian Constitution, *Article 21* states that no one shall be deprived of their life and personal liberty except by the procedure established by law. The right to privacy is implicit in this fundamental right. It also has the right to be let alone. The right to privacy in Article 21, should also be read with the right to publish any matter in public interest but subject to restrictions. Though the right to privacy is not directly mentioned as a fundamental right in the Constitution, it can be found that the Supreme Court has derived such right from A.21 as well as other provisions of Directive Principles of State Policy.

The recognition of the right to privacy in India started with *Kharak Singh v. State of Uttar Pradesh and others*[13]6 where the court held that as the constitution does not expressly declare the right to privacy as a fundamental right, it is an essential ingredient of personal liberty. Thereafter in *Gobind v. State of Madhya Pradesh and Another*[14], the right to privacy is incorporated under the right to life and personal liberty by

[10] AIR 264, 1994 SCC (6) 632
[11] AIR1997SC568
[12] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1
[13] AIR 1295, 1964 SCR (1) 332
[14] AIR 264, 1994 SCC (6) 632

the humanistic expansion of Article 21. In *R. Rajagopal v. State of Tamil Nadu*[15]8, the Supreme Court declared that the right to privacy has acquired a constitutional status and it is implicit in A.21. It is the "right to be let alone". A citizen can protect his privacy, his family, his personal life, childbearing, and other matters.

CASE LAWS:

Kharak Singh vs. the State of U. P. & Others, 18 December 1962:[16]

In this case, Kharak Singh was charge-sheeted for dacoity but was released due to lack of evidence. The police have subjected him to surveillance under Chapter XX of the UP police regulations. As part of this surveillance, there was secret monitoring of his house and approaches, night-time visits, and other inquiries about his life. He challenged this provision arguing that they violated his fundamental rights under Article 19(1)(f) and Article 21 of the Indian Constitution. The court ruled against domiciliary visits permitted by police regulation but held that the right to privacy is not explicitly included in the Constitution. But Justice Subba Rao contended that privacy is an integral part of personal liberty. Therefore, the Supreme Court gave mixed interpretations of privacy. The majority suggested that privacy was not a constitutional right while Justice Subba Rao said that it was. This case gave way to many future legal developments in the concept of privacy.

R. Rajagopal vs. State Of T.N on 7 October 1994[17]***:***

The petitioners wanted to publish an autobiography of Auto Shankar, who was a serial killer in prison. This autobiography revealed some of his connections with several state authorities. The main issue in this was whether writing an autobiography of a person without their consent would violate privacy. The court held that if something is posted about an individual's private affair without their permission, it can violate their right to privacy. The court also included an exception that if the information published is taken from a public record of an individual, it would not be an infringement of their privacy. This ruling aimed at balancing the right to privacy with the public's access to information in the public domain.

Mr. 'X' vs. Hospital 'Z', 21 September 1998:

In this case, the hospital had disclosed confidential information that the petitioner had AIDS which resulted in the cancellation of his marriage. The petitioner had the right to confidentiality of his health records. In this case, the court held that the right to confidentiality was not violated and it was revealed in public interest. This information was revealed to the fiancée so that she was informed about her prospective partner and the communicable disease he was suffering from. Hence the breach of confidentiality was justified to serve a public health purpose

***M. P. Sharma and Others vs. Satish Chandra, 15 March 1954*:**

Dalmia Group were facing allegations of fraud and a search warrant was issued under section 96(1) of the Code of Criminal Procedure to search the premises of the Dalmia Group. The Dalmia group challenged the search warrant, claiming it violated Article 20(2) of the constitution, which is protection against self-incrimination. The court said that a search cannot be considered an act of self-incrimination. The court said that search and seizure is a fundamental tool for the state to safeguard social security and is subject

[15] AIR 300, 1954 SCR 1077
[16] AIR 1295, 1964 SCR (1) 332
[17] AIR 264, 1994 SCC (6) 632

to legal regulation. The court upheld the authority of search and seizure and concluded that privacy could not be invoked as a defence against search and seizure.[18]

Justice K.S. Puttaswamy (Retd) vs. Union of India, 2017:[19]

This significant and landmark judgment was delivered in 2017. The Indian Supreme Court resolved the ambiguity relating to the right to privacy by establishing it as a fundamental right stemming from Article 21 of the Constitution. The court's judgment broadened the scope of privacy to encompass the privacy of one's body, mind, decisions, and information. However, it was also said that this right is not absolute and can be subject to restrictions by the state, provided it passes specific tests specified by the court. The tests include the test of legality, a test of a legitimate aim, and an examination of proportionality, as articulated in this judgment. This development was a crucial milestone in the evolution of privacy as a fundamental right in India, opening new facets in the legal landscape as privacy gained constitutional recognition and protection. It laid the foundation for many legal interpretations related to various aspects of privacy in the country.

Other legislations:

INFORMATION TECHNOLOGY ACT, 2000

The IT Act of 2000 is crafted for the protection of people from cyber-related crimes. Now that media is openly available to a large number of people, it is prone to being misused. This act defines different offences and its punishment. *Sections 65, 66, 66A, 54, 6C, 66D, 66E, 66F, 67, 67A* and *67B* under Chapter XI of the Act, contain the punishments for computer-related offences especially those committed through digital media. Some of the offences are identity theft, sending offensive messages to people, cheating by personation, transmitting obscene content, materials showing any person in a sexually explicit act etc.[20]The newly introduced *Section 43A* of the Act starts introducing a mandatory data protection regime. This section punishes with compensation, those who fail to protect data.

Punishment for violation of privacy is provided in *Section 66E* of the Act. It states that any act by a person who, knowingly or unknowingly, without consent, takes a photograph of the private areas of a person, sends such a photograph to someone else or publishes such a photograph, under circumstances which violate the person's privacy, will be considered a crime.[21]*Section 69* allows the central as well as the state government to direct the monitoring for interception or decrypting any information in the interest of sovereignty or integrity of the nation, defence, security, friendly relations with other countries, public order, prevent inciting serious offences or for investigation of an offence. *Section 69A* allows the central government to block access to certain information in the computers for similar reasons and issue directions for the same. Section 69B allows the Central Government to let some agencies monitor and collect data for cyber security.

This Act also provides the liability to intermediaries such as sites. The intermediaries are not responsible in certain cases but they will be if they encourage any kind of unlawful acts or fail to remove content after being told by the Government60. Intermediaries can also be punished if they contravene *section 69, 69A,69B*. *Section 70 B* establishes a national agency for cyber security, the Indian Computer Emergency

[18] AIR 300, 1954 SCR 1077

[19]

[20] Shishir Tiwari and Gitanjali Ghosh, 'Social Media and Freedom of Speech and Expression: Challenges before the Indian Law' SSRN (2014) 1 <http://dx.doi.org/10.2139/ssrn.2892537

[21] Cyberspace & Sexual Violence Laws' Safecity <https://www.safecity.in/cyberspace-sexual-violence-laws/>.

Response Team[22]. The government can also issue rules to control the collection, transfer and processing of data under the IT Act like the Information Technology Rules.

Section 66A of the act was held to be unconstitutional in the case of *Shreya Singhal v. Union of India*[23]. In *Delhi High Court v. Google LLC*, Google was asked to take down content which violated privacy and affected children. The court ordered Google to take down videos which made people to believe that Aradhya Bachan was critically ill and dead.[24]

CABLE TV ACT, 1995

Millions of posts are shared across the world every minute. It becomes a herculean task to ensure the safety of millions of users. The development of technology over the years has made the accessibility to the Internet at affordable rates. There are a variety of laws to regulate content. The Constitution guarantees the right to freedom of speech and expression under Article(1)(a). This right is not absolute and is subject to reasonable restrictions[25]. Laws introduced over the years, unrelated to media regulation, have restricted this fundamental right. Laws for media regulation are as follows

Cable television networks must follow programme rules and advertising codes provided under the Cable TV Act [26]. The code is given in Cable Television Network Rules,1994[27] and the programmes to be telecasted should fulfil certain requirements. For example, contents that offend "good taste or decency", or might incite violence or promote an "anti-national attitude", disparage women or children, or affect the "integrity of the nation", anything that contains obscene, defamatory, false or innuendos or half-truths are prohibited [28]. In the same way, advertising code restricts content and prescribes a time limit that advertisements can be displayed for an hour of content.

If the Authorised Officer under the Act, thinks it is in the public interest, if it does not abide by the rules or if it can promote enmity or disharmony amongst religious or linguistic groups, which is likely to disturb the public tranquillity, can prohibit a programme from being transmitted [29]. The Central Government can also prohibit cable TV networks in the public interest on specified grounds only [30]. If the programme code is violated, the Ministry of Information and Broadcast (MIB) can issue warnings, advisories or orders.[31] The breach of this act is punishable by fine or imprisonment or both.[32]. The MIB set up an Electronic Media Monitoring Centre in 2008 to monitor the content of TV channels and check the violations of the programme or advertisement code[33].

[22]Section 79(3) of The IT Act
[23] AIR 2015 SUPREME COURT 1523
[24] Ms. Aaradhya Bachchan And Anr vs Bollywood Time(2023)
[25] A 19(2), Constitution of India: "Nothing in sub clause (a) of clause (1) shall affect the operation of any existing law, or prevent the State from making any law, in so far as such law imposes reasonable restrictions on the exercise of the right conferred by the said sub clause in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality or in relation to contempt of court, defamation or incitement to an offence."
[26] Cable Television Networks (Regulation) Act, 1995, Sections 5 and 6.
[27] Cable Television Network Rules, 1994, Rules 6 and 7, "Programme and Advertising Codes", <available at https://mib.gov.in/sites/default/files/pac1.pdf>.
[28] Cable Television Network Rules, 1994, Rule 6.
[29] Cable Television Networks (Regulation) Act, 1995, Section 19.
[30] Cable Television Networks (Regulation) Act, 1995, Section 20.
[31]Cable Television Networks (Regulation) Act, 1995, Section 20.
[32] Cable Television Networks (Regulation) Act, 1995, Sections 16 and 17
[33] Ministry of Information and Broadcasting, "Monitoring of TV Channels- regarding", 22 July 2014, <mib.gov.in/sites/default/files/Letter_reg_Facilitation_of_Monitoring_of_TV_Channels_by_EMMC.pdf>.

DIGITAL PERSONAL DATA PROTECTION ACT, 2023

Data protection laws have been a priority across the world. After a 5-year long process, the Digital Personal Data Protection Act came into existence. With the rapid growth of technology, the Indian Parliament felt the need to establish legislation similar to the General Data Protection Regulation (GDPR). The Digital Personal Data Protection Act (DPDP)[34] came into force on 11th August 2023 after a long journey of discussions and negotiations. Personal data is defined under the DPDPA as "any data that relates to a natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, or an online identifier." This legislation makes India the 19th member of the G20 summit to establish a personal data protection act.[35] Six years after *Justice K.S. Puttaswamy vs. Union of India*[36], this act comes into existence. In this landmark case, Supreme Court recognised right to privacy within the context of the "right to life." The Indian Government was on a mission to protect personal data which lead to the DPDP Bill. The DPDP has drawn inspiration from the EU's General Data Protection Regulation (GDPR) and is quite broad. It applies to all kinds of groups, private as well as public. It lays down rules regarding how data is to be used and focuses only on personal data. DPDP also grants several rights like;

- The right to access their personal data
- The right to rectify inaccurate personal data
- The right to the erasure of their personal data
- The right to restrict the processing of their personal data
- The right to data portability
- The right to object to the processing of their personal data

The Data Protection Board of India ensures that the rules are followed and check complaints and impose fines. But they cannot create new rules nor can they give any advice.[37]This Act also has certain exceptions. Depending on the functions that Government bodies perform, they have certain exemptions. Personal data available to the public, data processed for research purposes, or personal data of foreigners in Indian companies also have certain exceptions. If notified by the government, certain startups are also exempted. The Act also provide powers to the Central Government to request personal data to entities and to issue rules like the regulations under US state privacy laws

CHALLENGES AND REFORMS

1. Legal challenge

In India even though there are a few proxy legislations on safeguarding privacy there is no proper legislation addressing all facets of privacy. Therefore, there are the following bugs in the legal regime:

1. There is no accord on the subject of privacy as there is no legitimate law that covers every nuance of privacy and sufficient measures to safeguard it.

[34] Digital Personal Data Protection Act (DPDP), https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf
[35] "News of the day: PM hits out at Opp at G20 meet, Digital Personal Data Protection bill now an act and more", The Telegraph, September 2023, https://www.telegraphindia.com/gallery/news- of-the-day-prime-minister-narendra-modi-hits-out-at-opposition-at-g20-meet-digital-personal-data-protection-bill-now-an-act-and-more-photogallery/cid/1958598?slide=1
[36] Justice K.S.Puttaswamy(Retd) vs Union Of India on 26 September, 2018
[37] Roy R., Zanfir-Fortuna G., The Digital Personal Data Protection Act of India, Explained, August 2023, Future of Privacy Forum. https://fpf.org/blog/the-digital-personal-data-protection-act-of-india-explained/#:~:text=The%20DPDP%20Act%20requires%20that,must%20be%20free%20to%20give

2. There is no distinction provided between public information, private information, or sensitive information.
3. There is a lack of proper standard of protocol in dealing with creating, processing, transferring, or storing data.
4. There is a significant lag behind on matters of cross-border information transmission.
5. There is a lack of adequate checks on data quality, proportionality, or transparency.

2. Technologic challenge:

The Information and Communications Technology (ICT) revolution and globalisation have transformed Indian information. It improved the portability and accessibility of information. Not just the corporate sector, but also the government sector. Even though, these have made our lives more convenient and quicker, the sweet fruit was the result of multiple mayhems making personal lives more public. Biometrics (fingerprints, hand geometry, face, voice, iris, and keystroke recognition), Smart cards, Wireless technologies, Location detection technologies (such as Global Positioning Systems), RFID, Voice over Internet Protocol (VoIP), Data-matching and data mining technologies, and Surveillance Technologies are some of the technologies that have the potential to impact privacy. With the recent advancements in technology, computers can now store and filter large amounts of data. Data matching is considered a huge threat, where the information collected is evaluated including personal information like personality, traits etc "Privacy shields us from abuses by those in authority, even if we're doing nothing wrong at the time of surveillance," explains security expert Bruce Schneier.[38]

12. A number of Internet security and privacy professionals say that "security doesn't exist" and that "privacy is dead-get over it." Cookies and site loggers have made private information more susceptible on the internet.

3. Political and social challenges:

According to the Information Technology principle, people are the weakest link in the chain of information protection. Major issues in this sector are:

1. Policymakers tend to neglect the technological arena therefore disregarding privacy. This is mainly because privacy is not a pinnacle issue in Indian society and is often inferior in priority.
2. International companies have made the Indian market their hub as it is cost-effective and they have no statutory obligations to follow regarding data safety.
3. Breach of trust between individuals is another prominent issue. The majority of family law cases are registered in this regard.
4. Encroachment of media into the life of an individual nullifying the boundaries of private space.
5. Increasing trends in the usage of social media networks like Instagram, Facebook, Twitter etc over the years have built vulnerability to the public analysis of personal lives, tarnishing privacy.

These challenges can be overcome by implementing adequate regulations addressing these issues. The government and policymakers should consider the dynamic technological advancements and personal interest weighing both equally.

CONFLICT OF STATE SURVEILLANCE AND PRIVACY INTRUSIONS

The government has consistently argued that content regulation is essential for maintaining public order,

[38] Bruce Schneier The Eternal Value of Privacy
http://www.wired.com/politics/security/commentary/securitymatters/2006/05/70886

curbing misinformation, and addressing issues like cybercrime and hate speech. However, critics have raised concerns that these regulations may lead to excessive censorship, stifling dissent and free speech, which are protected under Article 19(1)(a) of the Indian Constitution. The balancing act between content regulation and constitutional freedoms remains a subject of legal and public debate.

(a) Indian Jurisprudence

Justice K.S. Puttaswamy (Retd.) v. Union of India case

"Privacy is an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution".

This case is commonly known as the Right to Privacy Case. It is a landmark case decided by the Supreme Court of India. The case that emerged out of the raging concerns on the Aadhar issues redefined the relationship between the state and its citizens concerning privacy.

The facts of the case are that the Aadhaar program was initiated by the central government in 2009 to provide a unique identification number to Indian residents, based on their biometric data, such as fingerprints and iris scans. This programme aimed to rationalise the delivery of social welfare schemes and eliminate identity fraud. However, significant concerns were raised about its potential misuse for state surveillance and the risk of data breaches. The main concern was about the potential misuse of the data collected by the government without adequate safeguards which can lead to the violation of the right to privacy. The contentions worsened as the right to privacy was not a fundamental right then.

1. **Right to Privacy as a Fundamental Right**: a prominent question that arose in the court was the recognition of the right to privacy as a fundamental right.
2. **State Surveillance Concerns:** this case also examined the extend of state surveillance, which included data collection etc.
3. **Reasonable Restrictions**: The need for the rights to be reasonable and not absolute was also addressed in this case.

This case was historic in all aspects as a nine-judge bench of the Supreme Court unanimously recognized the right to privacy as a fundamental right under Article 2. The court held that Privacy is an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution and the state action infringing on this right must pass the tests of legality, necessity, and proportionality. While the judgment upheld the validity of the Aadhaar scheme in a later ruling (2018), it imposed strict limitations on its use, ruling that Aadhaar cannot be mandatory for services beyond state benefits and subsidies. It also prohibited private entities from using Aadhaar data, highlighting concerns about data privacy and surveillance.

This case has a huge impact on data privacy, state surveillance, and digital rights in India. This ruling subsequently paved the way for the drafting of the Personal Data Protection Bill. This case marks a turning point in Indian constitutional law, asserting that in the digital age, privacy is as crucial as any other fundamental right and must be protected against the overreach of state surveillance.

***(b)* American Jurisprudence**

The US Supreme Court case *Whalen v. Roe*[39] examined whether a state's data collection violated privacy rights but did not declare a right to informational privacy. The Court used a threefold proportionality test similar to one from the Indian Supreme Court in Puttaswamy, noting that there were safeguards against misuse of data. Unlike Aadhaar in India, Whalen had better protections against data abuse. Later, in *NASA*

[39] 429 U.S. 589 (1977)

v. Nelson[40], the Court ruled that a government background check requiring employees to reveal past illegal drug use did not violate any right to informational privacy. In *United States v. Jones*[41], Justice Sotomayor suggested that GPS tracking could violate privacy without trespassing, but the majority focused on trespass instead. Overall, US law has not clearly recognized a right to informational privacy under the Constitution, though the Whalen case provides some guidelines

(a) United Kingdom Jurisprudence

The Calcutta Committee Report defined "privacy" as the individual's right to be protected from intrusions into their personal life. The UK, which signed the *European Convention on Human Rights*, incorporated it into its law through the *Human Rights Act 1998*. *Article 8* of the Convention states that everyone has the right to respect their private and family life. However, individuals cannot directly claim a violation of privacy under this article in the UK. Court cases like *Campbell*[42] *and Vidal-Hall v. Google*[43] have allowed claims for misuse of private information. The UK Supreme Court identified two key aspects of this misuse: protecting confidentiality and preventing intrusion into privacy. An interim injunction can stop further disclosure of private information. The Data Protection Act 1998 also protects private information in the UK. The Court of Appeal ruled that individuals could seek compensation if their personal information is misused under this Act, including for emotional distress. While the UK doesn't use a proportionality test for privacy rights, the Privy Council's decision in Elloy de Freitas[44] established a three-step test for legislative actions affecting fundamental rights. It requires considering whether the legislative goal justifies limiting a right if the measures are connected to that goal, and if they are necessary to achieve it. The House of Lords added a fourth step about balancing societal interests with individual rights. The proportionality test used by the UK courts is similar to one accepted by India's Supreme Court but may allow the UK Parliament more leeway in creating surveillance programs due to its focus on societal interests over individual rights.

INDUSTRY PRACTICE ON DATA PRIVACY AND CONTENT REGULATION

India, being the largest digital market worldwide, faces an intricate landscape in terms of content regulation. The immediate and rapid surge of social media, digital platforms, and mobile internet has led to a diverse range of content varying from informative to harmful. To balance the imperatives of freedom of speech, public safety, and data privacy, the Indian government, tech companies, and legal frameworks have been shaping a dynamic regulatory environment.

1. Government Regulations

The Indian government has taken multiple initiatives in regulating content, particularly through the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. These rules provide the government with the power to demand the removal of certain content from social media platforms and streaming services if it violates public order, decency, or the sovereignty of the nation. grievance redressal mechanism was also introduced through which tech platforms were required to appoint grievance officers and ensure accountability.

2. Role of Tech Companies

Tech companies, especially global giants like Facebook, Twitter, Google, and WhatsApp, have become

[40] 131 S. Ct. 746, 751 (2011)
[41] 132 S. Ct. 945 (2012)
[42]Campbell v. MGN Ltd., [2004]
[43] UKHL 22 (2004)
[44] Elloy de Freitas v. Permanent Secretary of Ministry of Agriculture, Fisheries, Lands and Housing, [1999] 1 AC 69.

central to content dissemination in India. These platforms are required to comply with Indian laws, but they often face challenges in balancing government directives with their content moderation policies and user privacy standards.

WhatsApp, which is based on encrypted messaging, has faced pressure from the Indian government to allow traceability of messages to combat misinformation and fake news. However, WhatsApp has argued that this would compromise the privacy of users and undermine end-to-end encryption. Similarly, platforms like YouTube and Twitter must navigate the removal of content deemed harmful while facing accusations of either excessive censorship or insufficient regulation of offensive content.

CONCLUSION:

The idea of privacy is evolving in India. Lawmakers have started to value the importance of individual autonomy. In Europe, which is very proactive in managing personal data, there are strong rules to protect personal data, like the European Union's General Data Protection Regulation (GDPR). The GDPR has a comprehensive framework and has emerged as a benchmark for privacy legislation in many countries. India's approach is different, relying on contracts and some laws, especially as technology grows. India has an increasing emphasis on cybersecurity. The Digital Personal Data Protection Act (DPDP) has similarities to GDPR but also unique features, such as fewer reasons for data processing and broad exemptions for the government, government regulatory powers to refine the law and grant exemptions to certain parties, the absence of a predefined or heightened safeguard for special data categories, and an unusual provision allowing the government to request information from fiduciaries, the Data Protection Board, and intermediaries, as well as the ability to block public access to specific data on computer resources. The DPDP Act has been under development for a long period. More details will come when India sets up its Data Protection Board and makes more rules. The push for better data protection is influenced by new technologies and the recognition of privacy as a fundamental right by India's Supreme Court. There may be challenges at first, but as people see the benefits, data protection will likely improve in India. Overall, the future looks good for ordinary citizens.

REFERENCE:

1. Kumar, B. P., & Routh, B. (n.d.). What is privacy? The history and definition of privacy. Members' Reference Service, LARRDIS, Lok Sabha Secretariat, New Delhi. Prepared under the supervision of K. Sharma & C. N. Sathyanathan.
2. Lukács, A. (2023). What is privacy? The history and definition of privacy. Journal of Management & Public Policy, 15(1), 33-44. https://doi.org/10.47914/jmpp.2023.v15i1.003
3. Jha, S. (2020). Concept of privacy in India: A socio-legal critique. GIBS Law Journal.
4. Kalra, K. (2019). Right to privacy under Indian Constitution. Indian Constitutional Law Review, Edition VIII. Agradoot Web Technologies LLP.
5. Khamroi, A., & Shrivastava, A. (2021). Analysing the practical implications of a right to privacy: State surveillance and constitution. Centre for Research in Finance, Technology & Law Working Paper, No. 4/2021.
6. Sengupta, S., Giridhar, A. (n.d.). Political economy of communications and media regulation in India: Impact of laws on online curated content.

7. Ajay Kumar, 'Digital Media Regulations in India: Some Reflections' in Pawandeep Kaur (ed), Emergent Regulatory Governance: Key to Indian Regulatory Laws 303-337 (Indu Book Services Pvt Ltd, New Delhi 2022)
8. Statista. (n.d.). Content regulation in India. Retrieved from https://www.statista.com/topics/11824/content-regulation-in-india/#topicOverview.
9. PRS Legislative Research. (n.d.). Regulation of media in India: A brief overview. Retrieved from https://prsindia.org/theprsblog/regulation-of-media-in-india-a-brief-overview?page=43&per-page=1.
10. Endpoint Protector. (n.d.). India's personal data protection bill: What we know so far. Retrieved from https://www.endpointprotector.com/blog/indias-personal-data-protection-bill-what-we-know-so-far/.