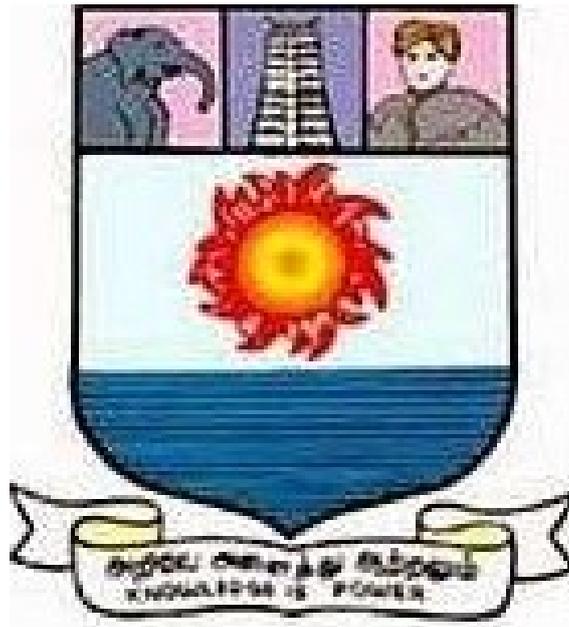


MANONMANIAMSUNDARANARUNIVERSITY

**Directorate of Distance and Continuing
Education**

Tirunelveli, 627012, Tamil Nadu



MA Journalism and Mass Communication

I Semester

Communication Laws

Self - Learning Material

Communication Laws - Elective						
Course Specific Objective						
<i>This course Communication Laws, provides an in-depth understanding of the Indian Constitution and its impact on communication laws.</i>						
Hours Per Week						Credits
Lecture	5	Tutorial	-	Practical	-	3
Unit-I: Indian Constitution						
<p>Foundations of the Indian Constitution. Indian Constitution from Communication Perspective Salient Features of The Indian Constitution. Importance of Articles 21 and 32. The Parliament-Directive Principles. Constitutional Amendments. Fundamental Rights and Duties- Article 19 1 (A)– Various Freedoms and Reasonable Restrictions Centre-State Relationship. State, Central and Concurrent List</p>						
Unit-II: Freedom of Speech and Expression						
<p>Concept of Positive and Negative Liberty. Free Speech and Private Properties. Press Freedom. Philosophy of Free Speech. Free Speech and Its Limits. Freedom of Press and Regulations. Hate Speech and Censorship in India. International Instruments on Free Speech and Expression. Social Media as an Alternate-Censorship in Social Media- Privatization of News Regulation- are Social Media Companies Platforms or Publishers. Shadow Banning. Algorithmic Downgrading in Recommender Systems.</p>						
Unit-III: Media-Related Acts and Regulations						
<p>Books and Registration Act. Registration of Newspapers Working Journalist Act. Press Council of India; Cinematograph Act. Press Council of India; Official Secrets Act-Journalistic Defence Obscenity and Pornography- Censorship. Privileges of Parliament. Defamation, Libel, Slander-Contempt of Court. Landmark Cases related to Media. Cases relating to freedom of expression and press Content Regulation in Broadcast News. Government Agencies, Trade Associations, Institutions related to Media Monitoring and Regulations-Ministry of I and B. Prasar Bharati, TRAI, INS, BARC.</p>						
Unit-IV: Intellectual Property Rights and Internet Governance						
<p>Intellectual Property Rights (IPR)- Concept of Innovation, Invention and Discovery. Intellectual Property Rights- Trademark, Patents, Geographical Indicators, and Secret and Confidentiality in IPR, Internet Governance International Conventions and Applications. WIPO. Copyright and Fair Use. Net Neutrality. (Facebook Basics Case) Various Government Notifications on social media and Internet Regulations. Internet Access and Broadband as Basic Rights. Role of Electronic Frontier Foundation (EFF) in Internet Governance. Social Media and other Digital Media/Platform Notifications of Government of India</p>						
Unit-V: Laws Related to Information						
<p>Cyber Laws and Legal and ethical aspects related to new technologies- AI/ML, IoT, Blockchain, Darknet and social media, Cyber Laws of other countries IT Act 2000 and its amendments. Limitations of IT Act 2000. Right to Information Act. Using RTI as a Reporting Tool.</p>						

Media and Privacy- Privacy Bill in India and in Other Countries. Right to Data Privacy-Relevant Sections of The IT ACT-Section 43A and Section 72 A. Sensitive Personal Data or Information) Rules, 2011 (“SPDI Rules”). Protection of Personal Information (PI) and Sensitive Personal Data and Information (SPDI)-Draft PDP Bill, 2019. Right to be Forgotten-Key Challenges and Debates. (EU’s Digital Services Act, 2023)

Course Specific Skills

provide a general orientation to learners on the Indian constitution, its history, and development	understand and apply the principles and laws of freedom of speech and viewpoint diversity.	provide orientation and examine legal issues and case laws related to media and journalism practices.	introduce and analyze intellectual property rights relevant to journalism practice in the Indian and global context.	recognize the ethical, legal, and socio-economic issues surrounding information and technology.
--	--	---	--	---

Reference Books

Key Textbooks

1. Powe, L. A., Jr. (2020). Media Law: A Very Short Introduction. Oxford University Press, Incorporated.
2. Mishra, A.K. (2020). Cyber Laws in India-Fathoming Your Lawful Perplex. Notion Press.
3. Stewart, D., & Stewart, D. R. (2017). Social Media and the Law: A Guidebook for Communication Learners and Professionals. Taylor & Francis.
4. Thomas, P. N. (2011a). Negotiating Communication Rights: Case Studies from India. SAGE Publications India.
5. Basu, D. D. (1986). Law of the Press. Prentice-Hall of India.

References

6. Belmas, G., & Overbeck, W. (2014). Major Principles of Media Law, 2015. Cengage Learning.
7. Bobbitt, R. (2015). Exploring Communication Law: A Socratic Approach. Routledge.
8. Lee, W. E., Stewart, D. R., & Peters, J. (2017). The Law of Public Communication. Routledge.
9. Caristi, D., & Davie, W. R. (2018). Communication Law: Practical Applications in the Digital Age. Routledge.
10. Caristi, D. G., Davie, W. R., & Cavanaugh, M. (2015). Communication Law. Routledge.

Web Resources

11. Harvard Journal of Law & Technology - <https://jolt.law.harvard.edu/>
12. Yale Journal of Law and Technology - <https://digitalcommons.law.yale.edu/yjolt/>
13. Journal of Media Law - <https://www.tandfonline.com/toc/rdml20/current>
14. Federal Communications Commission - <https://www.fcc.gov/>
15. World Intellectual Property Organization - <https://www.wipo.int/>
16. Civil Liberties Union - <https://www.aclu.org/>
17. Center for Democracy & Technology - <https://cdt.org/>
18. Media Law Resource Center - <https://www.medialaw.org/>

UNIT 1

INDIAN CONSTITUTION

Overview

- 1.1 Foundations of the Indian Constitution
- 1.2 Indian Constitution from Communication Perspective
- 1.3 The Indian Constitution
- 1.4 Salient features of the Indian Constitution
- 1.5 Article 21 of the Indian Constitution
- 1.6 The Indian Constitution's Article 32
- 1.7 Structure, Power and Functioning of Parliament
- 1.8 The Directive Principles of State Policy
- 1.9 Constitutional Amendments
- 1.10 Fundamental Rights
- 1.11 Fundamental Duties
- 1.12 Article 191 (A) – Various Freedoms and Reasonable Restrictions.
- 1.13 Centre-State Relationship
- 1.14 State, Central and Concurrent list.
- 1.15 Relationship between the Lists

Check your Progress

Glossary

Answers to Check Your Progress

Suggested Readings

OVERVIEW

In this unit, we will start with the introduction of the Communication law is a branch of the law that focuses on regulating the transfer of information through the computer, Internet, cable, satellite, telephone, and wireless communication. The People of India, having solemnly resolved to constitute India into a Sovereign Democratic Republic and to secure to all its citizens; Justice, social economic and political; Liberty of thought, expression, belief, faith and worship; Equality of status and of opportunity and to promote them among all.

Introduction

A constitution is an important document laying down the fundamental principles of a country. The country is governed by these principles. Laws are also formulated according to them. The constitution is regarded as the fundamental law of a country.

1.1 FOUNDATIONS OF THE INDIAN CONSTITUTION

Dr. B.R. Ambedkar, as the chairman of the Drafting Committee, stands out as the chief architect of the Indian Constitution, providing a robust framework to navigate the country's unique social, cultural, and religious diversity.

Adopted by the Constituent Assembly on November 26, 1949, and effective from January 26, 1950, the Indian Constitution enshrines unalterable basic principles that constitute its fundamental structure. These principles include:

- **Sovereignty and Republic:** Underlining that governmental authority emanates from the people, India remains free from external control.
- **Fundamental Rights:** Safeguarded by the Constitution, these rights serve as the foundation for framing laws in our democratic system.
- **Federalism:** Featuring a robust central government with states as subsidiary units, power flows from top to bottom.
- **Independent Judiciary:** As the third organ of government, the judiciary operates independently and impartially, handling all legal matters.
- **Secularism and Socialism:** Integral components added by the 42nd Amendment Act in 1976, these principles further fortify the Constitution's basic structure.

These five principles form the bedrock of the Indian Constitution, fortifying our democracy with the pillars of justice, liberty, equality, and fraternity. As a living document, the Constitution adapts to India's growth and transformations, ensuring its continued relevance.

1.2 THE INDIAN CONSTITUTION FROM COMMUNICATION PERSPECTIVE

The intricate relationship between the Indian Constitution and communication stands as a testament to the nation's unwavering commitment to democracy and fundamental rights. Adopted in 1950, the Constitution has been a guiding force in shaping a vibrant and diverse media landscape that plays a pivotal role in Indian society.

Upholding Freedom of Expression: At its core, the Constitution champions the right to freedom of speech and expression through Article 19(1)(a). This foundational right empowers individuals to engage in open discourse without undue government interference, fostering a media environment where journalists can fearlessly investigate, report, and comment on matters of public interest.

Establishing a Media Framework: The Constitution provides the legal basis for various media forms, including print, broadcast, and digital media. It empowers the government to enact laws promoting media diversity, responsible journalism, and safeguarding the rights of media personnel. This framework has nurtured a diverse media ecosystem, encompassing news outlets, opinion platforms, and entertainment channels.

Balancing Freedom with Responsibility: While championing freedom of expression, the Constitution recognizes the need for reasonable restrictions in the public interest (Article 19(2)). This delicate balance ensures that the media operates within a framework protecting both individual rights and societal interests.

The Supreme Court's Role: The Supreme Court serves as a guardian of free expression and media rights, interpreting and applying constitutional provisions. Through landmark judgments, the Court has upheld freedom of speech while balancing it with other rights and societal interests, shaping the media landscape and ensuring responsible practices.

Communication and Social Transformation: The Constitution's emphasis on communication has been instrumental in India's social transformation. A free media contributes to information dissemination, education, and awareness, empowering citizens to participate in democratic processes, demand accountability, and advocate for social justice.

Challenges and Future Directions: In the digital age, challenges like misinformation and corporate influence emerge. The Constitution's principles, including freedom of expression and media pluralism, remain vital in navigating these challenges. Media

literacy, fact-checking, and ethical journalism practices are essential to uphold the Constitution's ideals.

A Symbiotic Relationship: The Indian Constitution's framework for communication has fostered a vibrant media ecosystem, upholding the fundamental right to freedom of expression. As the media landscape evolves, the Constitution's principles will continue to ensure a responsible, informed, and inclusive environment. This symbiotic relationship will shape democratic discourse and empower citizens to meaningfully engage in the public sphere, reflecting the enduring strength of India's democratic values.

1.3 THE INDIAN CONSTITUTION.

The Constitution of India stands as a monumental liberal democratic document, holding the record as the world's largest written constitution. Crafted over nearly three years, it comprises 448 articles, 25 parts, 12 schedules, and has undergone 98 amendments. While parliamentary powers can modify its aspects, the basic structure is considered sacrosanct, with any law violating it deemed unconstitutional and invalid by the judiciary.

Drawing from various sources, the Indian Constitution extensively incorporates elements from the Government of India Act 1935, encompassing federalism, emergency provisions, judiciary intricacies, and more. It also borrows aspects such as fundamental rights from the American Constitution, the parliamentary form from the UK, federal structure from Canada, directive principles from Ireland, and fundamental duties from the Soviet Union.

The preamble succinctly encapsulates the constitution's ideals, declaring India as a sovereign, socialist, secular, democratic, and republic nation. Each term signifies a distinctive characteristic, emphasizing independence, socialism, religious equality, democratic governance, and an elected head of state.

While exhibiting federal features, the constitution also integrates unitary elements, allowing for a temporary shift to a unitary system during emergencies. The fundamental rights enshrined within it serve as a shield against arbitrary power, protecting individual and minority rights from potential majority oppression.

Opting for a parliamentary form of government, the constitution endorses majority party rule, a cabinet system, and the leadership of the Prime Minister at the central level

and Chief Ministers at the state level. It establishes a single citizenship, fostering unity and mobility across the nation.

An independent and integrated judicial system prevails in India, with the Supreme Court holding the highest position. All courts are bound by its decisions. Special provisions for Scheduled Castes and Tribes underline the constitution's commitment to the development and welfare of marginalized sections of society.

Emergency provisions grant the President authority to take extraordinary measures in the interest of national security, unity, and integrity. These provisions can be implemented selectively or across the entire country based on prevailing circumstances. The Indian Constitution, through its comprehensive framework, continues to be the guiding force in shaping the nation's governance and societal structure.

1.4 SALIENT FEATURES OF THE INDIAN CONSTITUTION

Every constitution aims to build up a political structure based upon certain principles and ideologies. Some of these principles vary from constitution to constitution. These variations are the product of varying conditions and circumstances that determine the very nature of a constitution. The Indian constitution is not an exception to this rule. The Indian constitution has its own characteristics. The theory, philosophy, and ideology that influenced the constitution of India were the result of the ideological background and philosophical knowledge of the members of the Constituent Assembly, which drafted the constitution. The most important ideological groups represented in the Constituent Assembly were the socialists, the Gandhians, and the rightists. The socialist groups were divided into two: the Marxist socialists and democratic socialists. Marxists advocated for the evolutionary reconstruction of society, while democrats wanted to transform society through peaceful parliamentary methods. Both these groups were opposed to the private ownership of the important means of production. The rightist group supported the interests of the bourgeoisie and landed class. The Gandhians criticized the capitalist mode of production. They wanted the renewal and promotion of village and small-scale industries. In the political field, they proposed a decentralized democracy based on self-sufficient village panchayats. All these ideologies have some influence on the constitution of India. Besides these ideological and philosophical commitments, the constitution of India continued the constitutional developments that took place under the British, retaining the basic precepts of the

Government of India Act 1935. Dr. Subhash Kashyap observes, “the constitution of India is a most comprehensive document. It is unique in many ways. It cannot be fitted into any particular model. It is a blend of the rigid and flexible, federal and unitary, and presidential and parliamentary. It attempts a balance between the fundamental rights of the individual on the one hand and the socio-economic interests of the people and security of the state on the other. It represents a via media between the principles of parliamentary sovereignty and judicial supremacy”.

The following are some of the salient features of the Indian constitution.

Longest Written Constitution: The Republic of India has a written and enacted constitution. The original constitution contains 395 Articles divided into 22 parts. In the later period, a number of amendments were made to the constitution. Provisions were either added or deleted. Even after these amendments, the Indian constitution still remains the largest written constitution in the world.

Popular Sovereignty: The Indian constitution upholds popular sovereignty. The will of the people prevails ultimately in the affairs of the state. The sovereignty of the people is proclaimed in its opening words itself. The preamble begins with the words “We the people of India.” Elections to the Indian parliament and state legislatures shall be on the basis of adult suffrage. Governments derive their authority from the people, who elect their representatives at regular intervals. The idea of popular sovereignty is affirmed in several places in the constitution.

Sovereign, Democratic, Republic: The preamble of the constitution declares that India is a sovereign democratic republic. The Dominion status established under the Independence Act of 1947 has been terminated, and India emerged itself as a completely independent, sovereign state. India is totally democratic because the real power emanates from the people. The word ‘Republic’ denotes that the state is headed by a president, elected indirectly by the people.

Rigid and Flexible: The Indian constitution is partly rigid and partly flexible. The procedure for the amendment of the Indian constitution is neither very easy, as in England, nor very rigid as in the USA. The Indian parliament has given the power to amend many provisions of the constitution by a simple majority, as required for general legislation. Some other provisions may be amended by a special majority of the Indian Parliament, i.e., a majority not less than 2/3 of the members of each house present and

voting, which again must be a majority of the total membership of the House. A very few provisions of the Indian constitution require further ratification of not less than $\frac{1}{2}$ of the state legislatures for their amendment.

Cabinet System of Government: The Indian constitution establishes the cabinet system of government both at the center and in the states. The governments should always be responsible to the respective popular chambers of legislatures. At the center, the Cabinet is composed of a Prime Minister and a number of ministers. The Cabinet is the policy-formulating and executing body of the government. An executive system always responsible to the popular chamber of the legislature is a contribution of Britain to the world.

Secular State: The commitment to the goal of 'secularism' has been spelled out in clear terms. The word 'secular' has been added to the preamble by the 42nd amendment of the constitution (1976). In India, there is no official or state religion. It treats all its citizens alike and gives them equal opportunities. The Indian constitution guarantees freedom of religion to all persons.

A Federal System with Unitary Bias: Normally, in India, the system of government is federal, but the constitution enables the federation to transform into a Unitary State. The constitution establishes a Federal polity with a division of powers. India has a written constitution, with a dual polity and division of powers between the center and states. There is also a provision for a Supreme Court, the guardian of the constitution. The Supreme Court decides all disputes that arise between the states and the center. Notwithstanding with all these features of a federal setup, the Indian constitution has a Unitary bias too. For example, after distributing the governmental powers in three lists: Union list, state list, and concurrent list, the residual subjects are left with the center, by which the center is made more powerful than the states. Even in matters relating to the concurrent list, the Union government has the final say. Besides that, the head of state (Governor) is appointed by the President and acts as the agent in the states. At any time, the center can declare an emergency in the states (Article 356) and can take over the administration of any state.

Universal Franchise: Article 326 ensures the adoption of Universal adult suffrage. It enables any citizen of India to cast his vote, without considering any caste, color, sex, qualification, or property, or the like. The suffrage in India is wider than that in Great

Britain and the U.S.A. The concept of popular sovereignty which underlies the declaration in the preamble would have been hollow unless the franchise were extended to the entire population. Another creditable point of the constitution is the abolition of communal representation. In the constitution, there was no reservation of seats except for the SCs and STs and for the Anglo-Indian community.

Compromise Between Judicial Review and Parliamentary Superiority: The Indian parliament is not as supreme as that of the British parliament. At the same time, the Indian judiciary is not as supreme as in the USA. The Indian constitution follows a via media between the two. The Indian constitution endows the judiciary with the power of declaring any law as unconstitutional if it is beyond the competence of the legislature or if it is in contravention of the fundamental rights guaranteed by the constitution. Major portions of the constitution are liable to be amended only by the parliament by a special majority; if the judiciary proves too obstructive, ultimately the fact remains that the legislature must be supreme and the judiciary must not interfere in such measures as social reforms.

No Double Citizenship: Double citizenship has not been provided for all citizens of India, even though India has a federal system of administration. In the USA, double citizenship has been provided. All Indians, irrespective of their domicile, enjoy single citizenship.

Impartial and Independent Judiciary: Democratic freedom is meaningful only in the presence of an impartial and independent judiciary. The framers of the Indian constitution were highly conscious of this fact. The judiciary of India is not an agent or subordinate of the Government of India. If the judiciary is subordinate or an agent of the government, it could not be trusted as an impartial interpreter of the constitution, and conflicts and controversies between the center and the states. These facts compelled the constitution-makers to adopt judicial independence as a basic principle of the Indian constitution.

Fundamental Rights: The constitution of India includes a separate chapter that guarantees fundamental rights to all citizens. These fundamental rights are justifiable and inviolable. They are binding on the legislature as well as the executive. A citizen of India has the right to seek the protection of the judiciary if any of the fundamental

rights are violated. Any parliamentary act or executive order can be declared null and void by the Supreme Court/High Courts if it violates any of the Fundamental Rights.

Fundamental Duties: Article 51 A (Part IV A) was incorporated into the Indian constitution in 1976 by the 42nd Amendment. It introduced fundamental duties, which cannot be judicially enforceable. This incorporation was an attempt to balance individual freedom with individual duties.

Directive Principles of State Policy: Another distinctive feature of the Indian constitution is the Directive Principles of State Policy. This feature has been taken from the Irish constitution. The philosophy behind the Directive Principles is that the state and its agencies are commanded to follow certain fundamental principles while they frame their policies. These principles are assurances to the people. At the same time, they are directions to the Government, both central and state. The precepts of Directive Principles are not justifiable and hence they are not enforceable by a court order. They are designed to serve as a guide for the Union Parliament and the state assemblies in framing new legislation.

Unamendable Basic Feature: The Indian constitution has a basic structure that cannot be amended. Democracy, federal and republican character, secularism, judicial review, the system of free and fair elections, etc., are some of the features that constitute the basic structure of the Indian Constitution. The constitution of India is remarkable for many outstanding features. These features distinguish it from other constitutions. There were members in the Constituent Assembly who criticized the constitution as a 'carbon copy of the Act of 1935,' as a 'paradise of lawyers,' as a 'borrowed constitution,' etc. But the fact that it has survived for more than sixty years belies the apprehensions of the critics.

1.5 ARTICLE 21 OF THE INDIAN CONSTITUTION

Article 21 of the Indian Constitution is widely regarded as one of the most pivotal fundamental rights, explicitly enshrining the right to life and personal liberty. This constitutional provision serves as a crucial safeguard against arbitrary deprivation of individuals' lives and freedoms by the State. The significance of Article 21 is underscored by its broad interpretation and the expansive protection it affords to various facets of human existence.

Types of Rights Under Article 21:

1. Right to Life:

- The right to life under Article 21 extends beyond mere physical existence to encompass the right to live with dignity.
- The State is obligated to ensure citizens' access to basic necessities like food, water, shelter, healthcare, and education.
- The Supreme Court has interpreted the right to life to include the right to healthcare, education, and a clean environment.

2. Right to Personal Liberty:

- The right to personal liberty safeguards individuals from arbitrary arrest and detention by ensuring that law enforcement has a valid reason for arrest.
- It mandates the prompt presentation of the arrested person before a court, preventing prolonged detention without trial.
- Individuals have the right to challenge their detention through a writ of habeas corpus, compelling the court to review the legality of the detention.

Judicial Interpretation:

1. Freedom from Arbitrary Arrest:

- Law enforcement must have a valid reason for arrest based on suspicion of a crime or the person's conduct.

2. Protection against Detention Without Trial:

- Individuals cannot be detained for more than 24 hours without being produced before a magistrate, safeguarding against torture or abuse.

3. Right to Habeas Corpus:

- A crucial legal recourse, individuals can challenge their detention in court, ensuring a thorough inquiry into the legality of the detention.

Case Law Evolution:

1. Early Cases:

- Early cases like *A.K. Gopalan v. State of Madras* initially suggested that the right to life and personal liberty was subject to reasonable restrictions imposed by law.

2. Expansive Interpretation:

- Subsequent cases, such as *Meneka Gandhi v. Union of India* and *Kharak Singh v. State of Uttar Pradesh*, expanded the scope of Article 21. The right to life was recognized to include fair procedures, and personal liberty included the right to privacy.

3. Recent Developments:

- Recent Supreme Court decisions have strengthened fundamental rights under Article 21, acknowledging the right to a clean environment, the right to education, and the right to dignity as inherent components of the right to life.

Importance and Significance:

• Cornerstone of Indian Democracy:

- Article 21 is considered a cornerstone of Indian democracy, symbolizing the nation's commitment to safeguarding human rights.

• Upholding Rights of Marginalized:

- The article has played a pivotal role in upholding the rights of marginalized and vulnerable sections of society.

In essence, Article 21 serves as a powerful legal instrument, continually evolving through judicial interpretation to protect the core principles of life, liberty, and dignity in the diverse fabric of Indian society.

1.6 THE INDIAN CONSTITUTION'S ARTICLE 32

In the event of a violation of fundamental rights as outlined in Part III of the Indian Constitution, Article 32 empowers citizens to approach the Supreme Court, serving as a guardian and guarantor of these essential rights. It provides a mechanism for individuals to seek redress for violations of their fundamental rights by filing complaints with the Supreme Court. While the Supreme Court has primary jurisdiction under Article 32, Parliament has the authority, through legislation, to confer similar powers on other courts within their local jurisdictions.

Father Dr. B.R. Ambedkar once emphasized the significance of Article 32, stating that it is the soul and heart of the Constitution without which the Constitution would be rendered null. This constitutional provision is considered essential for upholding the rights of Indian citizens.

Before 1950, only the High Courts of Calcutta, Bombay, and Madras had the authority to issue writs. However, Article 32 empowers the Supreme Court to issue instructions, orders, or writs, including habeas corpus, mandamus, prohibition, quo-warranto, and certiorari, among others. Article 226 extends the power to issue writs to all high courts in India, subject to the jurisdiction defined by Parliament. It's important to note that Court Martial, as per Article 33, exempts military tribunals from the writ authority of the Supreme Court and high courts.

The writs issued in India are based on English law and are known as "Prerogative writs." Some of the key writs include:

1. Habeas Corpus:

- Protects individuals from unlawful detention.
- Allows a court order to produce the detainee before the court.
- Cannot be suspended even during emergencies under Article 359.

2. Certiorari:

- Issued by higher courts to reverse judgments of lower courts.
- Corrects jurisdictional and legal errors.
- Can be issued against administrative authorities violating rights.

3. **Mandamus:**

- Directs a subordinate court, government officer, or institution to perform specific acts or duties.
- Cannot be used against private individuals.

4. **Quo-Warranto:**

- Issued against someone usurping a public office.
- Investigates the legality of a person's takeover of a public office.
- Cannot be used against private offices.

5. **Prohibition:**

- Given by a higher court to a subordinate court to prevent jurisdictional excess or absence.
- Applies to judicial and quasi-judicial authorities.

Previous Judgments Related to Article 32:

- In *Romesh Thappar vs State of Madras (1950)*, the Supreme Court emphasized Article 32 as a "guaranteed" remedy for enforcing fundamental rights.
- During the Emergency, in *Additional District Magistrate, Jabalpur vs SS Shukla (1976)*, the Supreme Court held that the right to constitutional remedies under Article 32 could be suspended during a national emergency.

Constitutional experts emphasize that the courts, especially the Supreme Court, play a crucial role in determining whether an intervention is justified in a matter, ensuring that people maintain confidence in the justice system as the ultimate remedy for rights infringement.

1.7 STRUCTURE, POWER AND FUNCTIONING OF PARLIAMENT

The Parliament is the supreme legislative body in most countries, typically organized into two chambers: the upper house and the lower house. The lower house is presided over by the Speaker, responsible for maintaining order and ensuring procedural rules are followed. The structure includes key roles such as:

1. Leader of the House:

- Head of the government in the lower house.
- Responsible for proposing legislation and leading the government's business.

2. Leader of the Opposition:

- Head of the largest opposition party in the lower house.
- Responsible for holding the government accountable and criticizing its policies.

3. Members of Parliament (MPs):

- Elected representatives representing the interests of constituents.

Powers of Parliament: Parliament holds various powers, including:

1. Power to Make Laws:

- Exclusive authority to enact laws; bills must pass both houses to become law.

2. Power to Scrutinize the Government:

- Involves mechanisms like question time, select committees, and debates.

3. Power to Hold the Government to Account:

- Can pass votes of no confidence, forcing the government to resign.

4. Power to Amend the Constitution:

- Complex process requiring a majority vote in both houses.

Functioning of Parliament: The parliamentary process typically involves:

1. Introduction of a Bill:

- Proposed legislation introduced in one chamber.

2. Debate and Amendments:

- Bill debated, and amendments may be made.

3. **Voting:**

- MPs vote on the bill; if majority favors, it moves to the other chamber.

4. **Repeat in the Other Chamber:**

- Process repeated in the second chamber.

5. **Approval by Head of State:**

- If both chambers pass the bill, it is sent to the Head of State for approval.

6. **Enactment into Law:**

- If approved, the bill becomes law.

Parliament's Role in Democracy: Parliament is vital in a democratic system, providing a platform for citizens to voice concerns and holding the government accountable. It is the sole legislative body with the authority to make laws. Additionally, Parliament scrutinizes the government's actions through various mechanisms, ensuring transparency and accountability.

In summary, Parliament is a cornerstone of democratic governance, serving as the primary legislative authority and a crucial check on the government's powers.

1.8 THE DIRECTIVE PRINCIPLES OF STATE POLICY

The Directive Principles of State Policy (DPSP) in the Indian Constitution are designed to ensure socio-economic justice for the people and establish India as a Welfare State. These principles serve as instructions and guidelines for the central and state governments. Some features of the Directive Principles include:

1. **Non-justiciability:**

- They are not justiciable, meaning they cannot be enforced by the courts.
- Despite being non-justiciable, they are fundamental in governing the country, and it is the duty of the state to apply them in legislation.

2. **Based on Socio-economic Rights:**

- Rooted in socio-economic rights guaranteed in the Constitution, such as the right to education, right to work, and right to property.

3. **Guidelines for Future Legislation:**

- Intended to be a guide for future legislation rather than immediate implementation.
- Aim to create conditions for citizens to lead a good life.

4. **Objective:**

- The main objective is to establish conditions for citizens to lead a good life.

5. **Found in Part IV of the Constitution:**

- Legal provisions related to DPSP are found in Article 36 to Article 51 in Part IV of the Indian Constitution titled 'Directive Principles of State Policy.'

Some specific Directive Principles include:

- Free legal aid to the poor and weaker sections of society.
- Provision for just and humane conditions of work and maternity relief.
- Prohibition of child labor.
- Prohibition of traffic in human beings and beggars.
- Promotion of international peace and security.
- Promotion of harmony and brotherhood among all the people of India.

The DPSPs draw inspiration from socialist, liberal, and Gandhian philosophies. They provide guiding principles for future legislatures and executives. The Indian Constituent Assembly engaged in debates on the directive principles from November 15, 1947, to October 17, 1949, ultimately adopting them as a crucial part of the Constitution after careful deliberation. Despite being non-enforceable by the courts, these principles play a vital role in shaping the socio-economic policies and governance of the country.

1.9 CONSTITUTIONAL AMENDMENTS

The Constitution of India has undergone 106 amendments since its adoption in 1950. The amendment process is intricate, requiring a special majority in both houses

of Parliament, and in some cases, the ratification of half of the state legislatures. There are three types of amendments:

1. Amendments by Simple Majority:

- Passed by a simple majority of members present and voting in each house of Parliament.

2. Amendments by Special Majority:

- Require a special majority of two-thirds of the members present and voting in each house of Parliament.

3. Amendments by Special Majority and Ratification:

- Require a special majority in Parliament and the ratification of half of the state legislatures.

Some significant amendments include:

1. The First Amendment:

- Added the right to freedom of religion to the Constitution.

2. The Third Amendment:

- Empowered Parliament to make laws regarding fundamental rights.

3. The Seventh Amendment:

- Introduced a new impeachment procedure for the President, Vice-President, and judges.

4. The Forty-second Amendment:

- Made substantial changes to the Constitution, enhancing the powers of the Prime Minister and President.

5. The Forty-fourth Amendment:

- Reversed several changes made by the Forty-second Amendment and restored the original text of the Constitution.

The purpose of amendments to the Constitution is to adapt it to the evolving needs of the country. This includes:

- **Protecting Fundamental Rights:**
 - Ensuring the preservation of fundamental rights for citizens.
- **Strengthening the Democratic Framework:**
 - Enhancing democratic processes and institutions.
- **Addressing Social and Economic Issues:**
 - Responding to changing social and economic dynamics.
- **Ensuring Smooth Functioning of the Government:**
 - Facilitating effective governance and administration.

The Constitution of India is considered a living document, capable of modification to meet the contemporary challenges and aspirations of the nation. Amendments play a crucial role in maintaining the relevance and effectiveness of the constitutional framework.

1.10 FUNDAMENTAL RIGHTS

The Fundamental Rights and Directive Principles of State Policy are the cornerstone of the Indian Constitution, representing the basic human rights guaranteed to all citizens. These rights are applied without discrimination based on factors such as race, religion, gender, etc. Fundamental Rights are enforceable by the courts, subject to certain conditions.

The founding fathers drew inspiration from various sources while incorporating Fundamental Rights in the Constitution, including the Bill of Rights of the American Constitution, the French Declaration of the Rights of Man, the Irish Constitution of 1935, and the Universal Human Rights Charter of the UNO.

Part III of the Constitution (Articles 12 to 35) outlines Fundamental Rights, which can be categorized into:

1. **Right to Equality (Articles 14 – 18):**
 - Ensures equal rights for everyone, irrespective of various factors, and prohibits discrimination.
2. **Right to Freedom (Articles 19 – 22):**

- Guarantees freedom of speech, expression, assembly, association, profession, and residence, subject to reasonable restrictions.

3. Right Against Exploitation (Articles 23 – 24):

- Prohibits traffic in human beings, forced labor, and employment of children in hazardous conditions.

4. Right to Freedom of Religion (Articles 25 – 28):

- Secular in nature, guarantees freedom of conscience, profession, practice, and propagation of religion.

5. Cultural and Educational Rights (Articles 29 – 30):

- Protects the rights of minorities to preserve their culture and provides for educational rights without discrimination.

6. Right to Constitutional Remedies (Articles 32 – 35):

- Ensures remedies if Fundamental Rights are violated, allowing citizens to approach the courts directly.

Features of Fundamental Rights:

- Different from ordinary legal rights in enforcement; can be directly approached to the Supreme Court.
- Some rights are available to all citizens, while others are for persons (citizens and foreigners).
- Not absolute rights; subject to reasonable restrictions for state security, public morality, decency, and friendly relations.
- Justifiable and enforceable by courts; can be amended by Parliament without altering the basic structure of the Constitution.
- Can be suspended during a national emergency, except rights under Articles 20 and 21.
- Application can be restricted in areas under martial law or military rule.

Fundamental Rights place limitations not only on the Union Government but also on the States and authorities with the power to make laws. Article 32 empowers the Supreme Court to issue writs for the enforcement of Fundamental Rights. The Constitution's 86th Amendment Act, 2002, made the Right to Education a Fundamental Right for children aged 6-14 years.

1.11 FUNDAMENTAL DUTIES

Fundamental Duties are moral obligations that every citizen is expected to fulfill to promote patriotism and uphold the unity of India. These duties are outlined in Part IV–A of the Constitution and focus on the responsibilities of individuals toward the nation. The Constitution prescribes the following Fundamental Duties for citizens:

1. To abide by the Constitution and respect its ideals and institutions, the National Flag, and National Anthem.
 2. To cherish and follow the noble ideals that inspired the national struggle for freedom.
 3. To uphold and protect the sovereignty, unity, and integrity of India.
 4. To defend the country and render national service when called upon to do so.
 5. To promote harmony and the spirit of common brotherhood, transcending religious, linguistic, and regional diversities; to renounce practices derogatory to the dignity of women.
 6. To value and preserve the rich heritage of our composite culture.
 7. To protect and improve the natural environment, including forests, lakes, rivers, and wildlife, and to have compassion for living creatures.
 8. To develop the scientific temper, humanism, and the spirit of inquiry and reform.
 9. To safeguard public property and abjure violence.
 10. To strive towards excellence in all spheres of individual and collective activity so that the nation constantly rises to high levels of endeavor and achievement.
 11. To provide opportunities for education to his child or ward between the age of six and fourteen years (this duty is specifically for parents or guardians).
-

These Fundamental Duties were added to the Constitution by the 42nd Amendment in 1976, and the 86th Amendment Act in 2002 introduced the duty of parents or guardians to provide education for children aged six to fourteen.

While the concept of Fundamental Duties was inspired by the constitution of the former USSR, it is noteworthy that the constitutions of the USA and several Western nations do not explicitly list fundamental duties. There have been suggestions to add more Fundamental Duties, such as the duty to vote in an election or the duty to pay taxes. However, any changes to the Fundamental Duties would require constitutional amendments.

1.12 ARTICLES 19(1)(A)-VARIOUS FREEDOM AND EXPRESSION

Article 19(1)(a) of the Indian Constitution guarantees to all citizens the right to freedom of speech and expression. This right is not absolute and is subject to reasonable restrictions imposed by law in the interests of the general public. The Supreme Court of India has held that the following are reasonable restrictions on the freedom of speech and expression:

- **Security of the State:** The government can impose restrictions on speech that it believes threatens the security of the State. This includes speech that incites violence, promotes terrorism, or reveals sensitive information about national security.
- **Friendly relations with foreign States:** The government can impose restrictions on speech that it believes harms India's friendly relations with foreign States. This includes speech that is offensive to foreign dignitaries or that threatens to disrupt international relations.
- **Public order:** The government can impose restrictions on speech that it believes threatens public order. This includes speech that incites violence, promotes hatred, or causes riots.
- **Decency and morality:** The government can impose restrictions on speech that it believes is indecent or immoral. This includes speech that is sexually explicit, promotes obscenity, or insults religious beliefs.
- **Contempt of Court:** The government can impose restrictions on speech that is in contempt of Court. This includes speech that scandalizes or prejudices the administration of justice.
- **Defamation:** The government can impose restrictions on speech that is defamatory. This includes speech that makes false statements about a person that damage their reputation.

The Supreme Court has also held that the following factors are relevant in determining whether a restriction on the freedom of speech and expression is reasonable:

- The nature of the speech: The Court will consider the severity of the speech and whether it is actually likely to cause harm.
- The context of the speech: The Court will consider the time, place, and manner in which the speech was made.
- The availability of alternative means of expression: The Court will consider whether there are other ways for the speaker to express their views without causing harm.
- The interests of the general public: The Court will balance the right to freedom of speech and expression with the interests of the general public.

In recent years, there has been a growing debate about the scope of the freedom of speech and expression in India. Some people argue that the government is imposing too many restrictions on the freedom of speech, while others argue that the government is not doing enough to protect public order and decency. The Supreme Court is likely to continue to play a key role in balancing these competing interests in the years to come.

1.13 CENTRE-STATE RELATIONSHIP

The Centre-State relationship in India is a critical aspect of its federal structure. Here are some key points to summarize the dynamics:

1. **Federal Constitution:** India follows a federal system where powers are divided between the central government and state governments. The Constitution clearly delineates the powers and functions of each level of government.
2. **Legislative Relations:** Legislative powers are distributed among the central and state governments through Union List, State List, and Concurrent List. This division helps prevent conflicts and ensures that each level of government can legislate on specific subjects.
3. **Executive Relations:** The execution of laws is divided between the central and state governments. While the central government can execute laws on subjects in the Union List, state governments have the power to execute laws on subjects in the State List. Concurrent List subjects see shared execution.
4. **Financial Relations:** Financial powers and resource distribution are crucial aspects. The central government collects taxes and has the power to borrow,

while state governments also collect taxes but often depend on financial assistance from the central government.

5. **Challenges:** Challenges in Centre-State relations include disputes over the division of power, distribution of resources, and the role of the central government in monitoring state activities. Disagreements on these issues can lead to tensions and conflicts.
6. **Recent Developments:** Recent developments include the rise of regional parties, the implementation of the Goods and Services Tax (GST), increased judicial intervention by the Supreme Court, and a changing political landscape. These factors have impacted the dynamics of Centre-State relations.
7. **Rise of Regional Parties:** Regional parties have gained prominence in Indian politics, influencing the power dynamics between the central government and the states.
8. **Goods and Services Tax (GST):** The introduction of GST, a unified tax system, has had a significant impact on the financial relations between the central and state governments.
9. **Judicial Intervention:** The Supreme Court has played an active role in resolving Centre-State disputes, influencing the balance of power between the two levels of government.
10. **Future Outlook:** The future of Centre-State relations remains uncertain, but it is expected to be a key issue in Indian politics. The ongoing evolution of these relations will shape the functioning of the federal structure in the country.

In conclusion, the Centre-State relationship is a dynamic and evolving aspect of India's governance, marked by both cooperation and tension. The effective functioning of the federal structure requires continuous efforts by both levels of government to find common ground and address the diverse needs of the nation.

1.14 STATE, CENTRAL AND CONCURRENT LIST

The Union List, State List, and Concurrent List are essential components of the Seventh Schedule in the Indian Constitution, providing a framework for the division of legislative powers between the Union government and the state governments.

1. Union List:

- **Nature:** The Union List is a list of subjects exclusively under the jurisdiction of the Union government.

- **Significance:** It includes subjects vital for the smooth functioning of the central government and matters that require uniformity across the nation.
- **Examples:** Defense, foreign affairs, atomic energy, and trade and commerce fall under the Union List.
- **Exclusive Power:** The Union government has exclusive power to legislate on these subjects.

2. State List:

- **Nature:** The State List comprises subjects exclusively under the jurisdiction of the state governments.
- **Significance:** It includes matters of local or regional importance, allowing state governments to address the specific needs of their citizens.
- **Examples:** Public order, police, education, and agriculture are part of the State List.
- **Exclusive Power:** State governments have exclusive power to legislate on subjects in the State List.

3. Concurrent List:

- **Nature:** The Concurrent List includes subjects of shared interest between the Union government and state governments.
- **Significance:** These subjects require cooperation and coordination between the central and state governments.
- **Examples:** Criminal law, marriage and divorce, bankruptcy and insolvency are subjects in the Concurrent List.
- **Shared Power:** Both the Union and state governments have the power to legislate on Concurrent List subjects.
- **Precedence:** In case of a conflict between a Union law and a State law on a Concurrent List subject, the Union law prevails if it is necessary in the national interest.

The Seventh Schedule, with its three lists, ensures a balanced and cooperative division of legislative powers, allowing both the Union and state governments to function effectively while addressing the diverse needs of the nation. The framework provides flexibility and adaptability to meet the evolving challenges and priorities of the country.

1.15 RELATIONSHIP BETWEEN THE LISTS

The Union List and the State List within the Seventh Schedule of the Indian Constitution serve as exhaustive catalogs, delineating the exclusive domains of legislative authority for the Union government and state governments, respectively. Their exhaustive nature implies that any subject not explicitly enumerated on either list is automatically relegated to the residual powers of the Union government. In essence, this confers upon the Union government the authority to legislate on these residual subjects, even if they aren't expressly mentioned in the Constitution.

In contrast, the Concurrent List is intentionally non-exhaustive, signifying that while certain subjects are specified, there may still be additional matters of mutual interest to both the Union government and state governments that are not explicitly listed. In such instances, a collaborative approach is adopted, allowing both the Union government and the state governments to share legislative power on these unenumerated but mutually relevant subjects.

The process of amending the Union List, State List, and Concurrent List is a constitutional prerogative. To bring about changes in these lists, a constitutional amendment is requisite. This demands a two-thirds majority in both houses of Parliament and the ratification of half of the state legislatures, ensuring a deliberative and inclusive process.

Examples of subjects found within each list illustrate the distinctive purviews of the Union government, state governments, and the shared responsibilities between them:

- **Union List:** Defense, foreign affairs, finance, currency and coinage, communications, railways, civil aviation, atomic energy, trade and commerce.
- **State List:** Public order, police, prisons, education, health, agriculture, irrigation, land revenue, forests.

- **Concurrent List:** Criminal law, civil procedure, marriage and divorce, contracts, trusts and trustees, copyright and patents.

This structured division of legislative powers is fundamental to maintaining a delicate balance between the centralized authority of the Union and the autonomy of individual states, promoting the principles of cooperative federalism in the Indian constitutional framework.

Check Your Progress

1. ----- of the constitution consists of the ideals, objectives and basic principles of the Constitution.

2. ----- chairman of its Drafting Committee, is considered the chief architect of the Indian Constitution.
3. ----- written and detailed constitution.
4. ----- is the presiding officer of the lower house.

Glossary

1. **Demonetization:** This is when a social media platform removes advertising from a user or piece of content.
2. **Federalism-** India has a strong central government with states as subsidiary units. The power flows from top to bottom.
3. **Members of Parliament (MPs):** MPs are elected representatives of the people. They represent the interests of their constituents in the chamber.
4. **Habeas corpus** mean document safeguards a person against being unlawfully detained.
5. **The preamble** of the constitution consists of the ideals, objectives and basic principles of the Constitution.

Answer to check your progress

1. Press
2. Shadowbanning
3. Hybrid model
4. Global reach

Suggested Readings

<https://www.open.edu/openlearn/mod/oucontent/view.php?printable=1&id=1747>

<https://www.cambridge.org/core/journals/pmla/article/abs/platform-or-publisher/C59144B77FC9FDD8674E3CB8C1675309>

<https://ro.ecu.edu.au/cgi/viewcontent.cgi?article=7853&context=ecuworks3>

UNIT 2**FREEDOM OF SPEECH AND EXPRESSION**

Overview

- 2.1 Liberty
- 2.2 Free Speech and private properties
- 2.3 Press Freedom
- 2.4 Philosophy of free speech and its limits
- 2.5 Freedom of Press and Regulations
- 2.6 Hate Speech and censorship in India
- 2.7 International instruments on free speech and expression
- 2.8 Social Media as an Alternate
- 2.9 Censorship in Social Media
- 2.10 Privatization of News Regulation
- 2.11 Social Media Companies Platforms or Publishers
- 2.12 Shadow banning
- 2.13 Algorithmic Downgrading In Recommender Systems.

Check your Progress

Glossary

Suggested Readings

Answers to Check Your Progress

2.1 Liberty

- Liberty can be defined as the freedom to do whatever one wants or the positive power of doing and appreciating the value of one's work.
- In modern politics, liberty is defined as the state of being free within society from control or oppressive restrictions imposed by authority on one's way of life, behavior, or political views.
- The exercise of liberty is contingent on capability and is constrained by the rights of others. Thus, liberty entails using freedom responsibly under the rule of law without depriving anyone else of their freedom.

Negative Liberty and Positive Liberty

The focus areas of Negative Liberty and Positive Liberty are different.

- Positive liberty is concerned with the freedom of an individual within the framework provided by society; it tends to enable the development of that society.
- Negative liberty is concerned with the areas of non-interference and domains of life of an individual that must not be violated.

Negative Liberty

- Negative liberty is the minimum non-interference area. It seeks to define and defend a zone of inviolability for the individual.
- It is concerned with explaining the concept of “liberty.”
- It recognizes that human nature and human dignity require a space where people can act freely.
- It explains that to express oneself, one requires non-interference and areas where individual liberties are not violated.
- Negative liberty, in contrast to positive liberty, is primarily concerned with freedom from external restraint.

Positive Liberty

- Positive liberty is the ability to act on one’s free will, as opposed to negative liberty, which is freedom from external restraint on one’s actions.
- Positive liberty may also refer to freedom from internal constraints.
- The idea of ‘freedom to’ is something that positive liberty is concerned about.
- Discussions of positive liberty with a long tradition can be traced to Rousseau, Hegel, Marx, Gandhi, Aurobindo, etc.
- Positive Liberty considers the nature of the relationship and conditions that exist between the individual and society.

- It is also about improving these conditions so that there are very few impediments to the development of the individual personality.
- Positive Liberty looks at the nature of the relationship and conditions between the individual and society.
- It is also about improving these conditions so that there are very few constraints in the way of the development of the individual personality.
- The benefit of enabling favorable conditions in material, political, and social domains is needed for an individual to develop his or her capability. For example, poverty or unemployment must not be the constraints for a person to have adequate material resources to pursue their wants and needs.

Freedom of Expression

- Freedom of expression is a fundamental value, and society must be willing to bear some inconvenience to protect it from those who seek to restrict it. Freedom of Expression is considered to belong to the minimum area of ‘non-interference.’
- John Stuart Mill, a political mastermind in 19th century Britain, offered a passionate defense of freedom of expression, including freedom of thought and discussion.
- The four reasons he gives for why there should be the right to express oneself in any case, for those who hold ‘false’ beliefs.
 1. Any idea cannot be entirely false: there is always some truth in what appears to us to be false. If we prohibit ‘false’ ideas, we risk losing elements of truth in them.
 2. Truth never emerges on its own: it emerges as a result of a conflict between opposing viewpoints. At the moment, the ideas that appear to be incorrect may have been valuable in the emergence of what we consider to be correct ideas.
 3. Conflict of ideas is always valuable: truth is always in danger of being reduced to an unthinking cliché. Only after we expose it to various points of view will we be able to trust it.

4. Associated uncertainties with actual truth: Thoughts that were thought to be false at one point in time often turn out to be correct later on. A society that suppresses all unsuitable ideas today risks losing significant knowledge.

Banning Creative Freedom

- A distinction is made between ‘negative liberty and positive liberty,’ and we recognize the need for ‘justifiable constraints,’ but these have to be supported by proper procedures and important moral arguments.
- Freedom granted under the freedom of expression is typically under attack by the people who want to restrict it. Hence, society must be ready to tackle such a possibility.
- The long-term prospects of Banning: Once one begins to ban, then one develops a habit of banning.
- When constraints are backed by organized social, religious, or cultural authority or by the might of the state, they restrict our freedom in ways that are difficult to fight against.

Liberalism

- Liberalism has been identified with tolerance as a value in political ideology.
- The rights of a person to hold and express his/her opinions and beliefs, even when they disagree with them, are often defended by liberals.
- Priority is given to individual liberty over values like equality by Liberals.
- Since ancient times, liberalism favored the free market and a minimal role for the state.
- However, present-day liberalism acknowledges a role for the welfare state and accepts the need for measures to reduce both social and economic inequalities.

2.2 FREE SPEECH AND PRIVATE PROPERTIES

The relationship between free speech and private property is complex and often contentious. On one hand, free speech is a fundamental right enshrined in many constitutions worldwide, essential for a healthy democracy, allowing individuals to express their views without fear of reprisal. On the other hand, property owners also have rights, including controlling access to their property and regulating activities taking place there.

In the United States, the First Amendment protects freedom of speech, but this protection is not absolute. The government can restrict speech in certain circumstances, such as incitement to violence or hatred. Moreover, the First Amendment does not apply to private property, allowing owners to generally prohibit speech on their premises, even if protected elsewhere.

Exceptions to this rule exist; for instance, the government may regulate speech on private property if deemed a public nuisance. Some states also have laws protecting free speech on specific private properties, like shopping malls.

The balance between free speech and private property rights is delicate. Protecting free speech is crucial for democracy, yet respecting property owners' rights is equally important. There's no easy answer, and the debate is likely to persist.

- The right to free speech is not the only consideration; property owners also have the right to privacy and control over their property.
- The balance between free speech and private property rights may vary based on the context, with stronger cases for free speech on publicly accessible private property.
- Striking a balance that protects both free speech and private property rights is challenging but essential for a healthy society.

2.3 PRESS FREEDOM

Press freedom in India is a complex issue despite constitutional guarantees. While Article 19(1)(a) grants freedom of speech and expression, the media faces challenges like self-censorship, government interference, and violence against journalists.

Legal Framework

India's constitution considers the press the fourth pillar of democracy. However, it allows reasonable restrictions on freedom of speech for national security, public order, and morality. These restrictions, including sedition and defamation laws, have been used to curtail press freedom. Indirect methods like advertising boycotts and tax raids are also employed by the government.

Self-Censorship

Journalists in India often self-censor due to fear of legal action, violence, or economic consequences. This hampers press freedom by discouraging reporting on sensitive topics.

Violence Against Journalists

India is among the most vulnerable countries for journalists, with many unsolved cases of violence. Recent years have seen a decline in press freedom due to increased politicization, rising nationalism, and intolerance of dissent.

Press freedom in India faces challenges, with constitutional guarantees undermined by self-censorship, government pressure, and violence against journalists. The future depends on upholding constitutional commitments and fostering an environment for journalists to work freely.

2.4 PHILOSOPHY OF FREE SPEECH AND ITS LIMITS

The philosophy of free speech is intricate, emphasizing the right to express oneself for a democratic society. Arguments for free speech include its role in pursuing truth, fostering individual autonomy, and contributing to a healthy democracy. However, concerns about the spread of harmful ideas and the potential for powerful voices to dominate lead to arguments for limitations on free speech in certain circumstances.

Arguments Against Unrestricted Free Speech

Unrestricted free speech can spread harmful ideas, such as hate speech and false information. Some argue for limitations, like banning hate speech or regulating false information, to prevent negative consequences.

The Balance Between Free Speech and Other Rights

Balancing free speech with other rights is complex and context-dependent. Free speech is not absolute and can be limited when conflicting with rights like freedom from violence or discrimination. Striking a balance is challenging but essential for a just society.

The philosophy of free speech is crucial for understanding democratic rights and responsibilities. Despite potential drawbacks, finding a balance that protects free speech while upholding other rights and values is essential.

2.5 FREEDOM OF PRESS AND REGULATIONS

Freedom of the press in India is legally protected by constitutional amendments, maintaining a hybrid legal system for independent journalism. Although not explicitly mentioned, it falls under freedom of speech and expression, granting media rights similar to those of citizens.

Rights of the Media

The press, considered the fourth pillar of democracy, has rights like defamation, freedom of speech and expression, publishing, receiving information, conducting interviews, reporting court proceedings, and advertising. However, Article 19(2) allows restrictions in the interest of sovereignty, security, public order, decency, morality, contempt of court, defamation, and incitement to offense.

Importance of Freedom of the Press in India

- Free exchange of ideas: Inspires critical thinking beyond social norms.
- Holding accountability: Ensures justice by bringing issues to public attention.
- Voice of the people: Represents majority thoughts, focusing on suppressed issues.
- Fourth pillar of democracy: Independently challenges the government, complementing other branches.

Current State of the Press

Despite progress, the current situation is challenging. Issues like fake news, paid news, biased media, and crimes against journalists persist, affecting the media landscape negatively.

Regulation of the Press

While the press in India mostly self-regulates, statutory bodies like the Press Council of India (PCI) exist to set guidelines and standards. However, criticisms highlight limitations in enforcing these guidelines, particularly concerning penalties for violations. The PCI's jurisdiction is limited to print media, leaving a need for effective self-regulation mechanisms that balance press freedom and social responsibilities, especially in electronic media.

2.2 FREE SPEECH AND PRIVATE PROPERTIES

The relationship between free speech and private property is a complex and often contentious one. On the one hand, free speech is a fundamental right enshrined in many constitutions around the world. It is essential for a healthy democracy and allows individuals to express their views and beliefs without fear of reprisal. On the other hand, property owners also have rights, including the right to control who comes onto their property and what activities take place there.

In the United States, the First Amendment to the Constitution protects freedom of speech. However, this protection is not absolute. The government can restrict speech in certain circumstances, such as when it incites violence or hatred. Additionally, the First Amendment does not apply to private property. This means that property owners can generally prohibit speech on their property, even if it is protected by the First Amendment in other contexts.

There are exceptions to this rule. For example, the government may be able to regulate speech on private property if it is deemed to be a public nuisance. Additionally, some states have laws that protect free speech on certain types of private property, such as shopping malls.

The balance between free speech and private property rights is a delicate one. On the one hand, we want to protect the right to free speech, which is essential for a democracy. On the other hand, we also want to respect the rights of property owners. There is no easy answer to this question, and it is likely to continue to be debated for many years to come.

- The right to free speech is not the only right that needs to be considered. Property owners also have the right to privacy and the right to control their own property.
- The balance between free speech and private property rights may vary depending on the context. For example, there may be a stronger case for allowing free speech on private property that is open to the public than on private property that is not.
- It is important to find a balance that protects both free speech and private property rights. This can be a difficult task, but it is essential for a healthy society.

2.3 PRESS FREEDOM

Press freedom in India is a complex and multifaceted issue. While India's constitution guarantees freedom of speech and expression, the country's media landscape is often characterized by self-censorship, government interference, and violence against journalists.

Legal Framework

The Indian Constitution's Article 19(1)(a) guarantees freedom of speech and expression to all citizens. This right extends to the press, which is considered to be the fourth pillar of democracy. However, the constitution also allows for reasonable restrictions on freedom of speech, including restrictions imposed in the interests of national security, public order, and morality.

In practice, these restrictions have been used to curtail press freedom. For example, the Indian Penal Code (IPC) contains a number of provisions that can be used to silence critical journalism, such as the sedition law and the defamation law. Additionally, the government has been accused of using indirect means to pressure the media, such as through advertising boycotts and tax raids.

Self-Censorship

Many journalists in India practice self-censorship in order to avoid harassment or reprisals from the government or other powerful actors. This can be a result of a fear of legal action, physical violence, or economic hardship. Self-censorship can have a

chilling effect on freedom of the press, as it can prevent journalists from reporting on sensitive or controversial topics.

Violence Against Journalists

India is one of the world's most vulnerable countries for journalists. According to the Committee to Protect Journalists (CPJ), at least 92 journalists have been killed in India since 2022. In many cases, these killings are never properly investigated or prosecuted.

Recent Developments

In recent years, press freedom in India has been on a downward trajectory. The country has slipped in the Reporters Without Borders (RSF) World Press Freedom Index, ranking 161st out of 180 countries in 2023. This decline is due to a number of factors, including the increasing politicization of the media, the rise of Hindustan nationalism, and the government's growing intolerance of dissent.

Press freedom in India is a fragile and hard-won right. While the country's constitution protects freedom of speech and expression, this right is often undermined by self-censorship, government interference, and violence against journalists. The future of press freedom in India will depend on the country's ability to uphold its constitutional commitments and to create an environment in which journalists can work freely and without fear.

2.4 PHILOSOPHY OF FREE SPEECH AND ITS LIMITS

The philosophy of free speech is a complex and nuanced one, with a rich history and a multitude of perspectives. At its core, free speech is the right to express oneself without fear of reprisal or punishment. This right is essential for a free and democratic society, as it allows for the exchange of ideas, the pursuit of truth, and the participation in public discourse.

Arguments in Favour of Free Speech

There are many arguments in favour of free speech. One of the most common is that it is necessary for the pursuit of truth. In order to find the truth, we need to be able to hear all sides of an issue, even those that we disagree with. Free speech allows

for the open exchange of ideas, which can help us to test our beliefs, challenge our assumptions, and ultimately arrive at a better understanding of the world.

Free speech is also important for individual autonomy and self-expression. Each person has the right to form their own opinions and beliefs, and to express them freely without interference from others. This right is essential for our sense of identity and our ability to participate in society.

Finally, free speech is a vital component of a healthy democracy. In order for a democracy to function properly, citizens need to be able to express their views and participate in the political process. Free speech allows for the open exchange of ideas, which can lead to informed decision-making and a more accountable government.

Arguments Against Unrestricted Free Speech

The unrestricted free speech can lead to the spread of harmful or dangerous ideas. For example, hate speech can incite violence or discrimination, and false or misleading information can lead to poor decision-making.

Another concern is that unrestricted free speech can give too much power to those who have the loudest voices. In a world where everyone is free to say whatever they want, the voices of the most powerful and privileged may tend to drown out the voices of the less powerful. This can lead to a society that is unfair and unjust.

As a result of these concerns, some people argue that free speech should be limited in certain circumstances. For example, they may argue that hate speech should be banned, or that false or misleading information should be regulated.

The Balance Between Free Speech and Other Rights

The question of how to balance free speech with other rights is a complex one that has been debated by philosophers and policymakers for centuries. There is no easy answer, as the appropriate balance will vary depending on the specific circumstances.

In general, however, it is important to remember that free speech is not an absolute right. It can be limited when it comes into conflict with other important rights, such as the right to be free from violence or discrimination.

The challenge is to find a balance that protects free speech while also protecting other important rights and values. This is a delicate task, but it is essential for a just and equitable society.

The philosophy of free speech is a rich and complex one that is essential for understanding our rights and responsibilities as citizens in a democracy. While there are many strong arguments in favor of free speech, there are also potential drawbacks that need to be considered. The challenge is to find a balance that protects free speech while also protecting other important rights and values.

Free speech is the right to express oneself without fear of reprisal or punishment. This right is essential for a free and democratic society, as it allows for the exchange of ideas, the pursuit of truth, and the participation in public discourse.

Free Speech and its Limits

However, free speech is not an absolute right. It can be limited when it comes into conflict with other important rights, such as the right to be free from violence or discrimination.

Here are some of the limits of free speech:

Incitement to violence: Speech that incites violence is not protected by the First Amendment. For example, if someone calls for violence against a particular group of people, this could be considered incitement to violence and could be prosecuted.

True threats: True threats are also not protected by the First Amendment. A true threat is a statement that is intended to cause someone to fear for their safety. For example, if someone threatens to kill another person, this could be considered a true threat and could be prosecuted.

Fighting words: Fighting words are not protected by the First Amendment. Fighting words are words that are likely to provoke an immediate violent reaction. For example, if someone calls someone else a racial slur, this could be considered fighting words and could be prosecuted.

Child pornography: Child pornography is illegal and is not protected by the First Amendment. Child pornography is any visual depiction of a sexually explicit act involving a minor.

Obscenity: Obscenity is not protected by the First Amendment. Obscenity is material that appeal to a prurient interest in sex, that depicts sexual conduct in a patently offensive way, and that lacks serious literary, artistic, political, or scientific value.

These are just a few of the limits of free speech. The specific limits of free speech vary from country to country and from court to court.

It is important to note that the limits of free speech are often controversial. Some people believe that free speech should be absolute, while others believe that it should be more limited. There is no easy answer to this question, as it depends on a variety of factors, such as the specific context and the competing interests involved.

Despite the limits, free speech is a vital right that must be protected. It is essential for a healthy democracy and for the pursuit of truth

Free speech is the right to express oneself without fear of reprisal or punishment. This right is essential for a free and democratic society, as it allows for the exchange of ideas, the pursuit of truth, and the participation in public discourse.

2.5 FREEDOM OF PRESS AND REGULATIONS

Freedom of the press in India is legally protected by the Amendment to the constitution of India, while the sovereignty, national integrity, and moral principles are generally protected by the law of India to maintain a hybrid legal system for independent journalism.

What are the Rights of the Media?

Freedom of the Press is nowhere mentioned in the Constitution. It is believed to be covered under Freedom of Speech and Expression. Hence, the rights of a common citizen are the same as the rights of a media or press house.

The media has certain rights to challenge the government and showcase the issues gaining rapid attention by the people through various media sources and houses. Some rights are:

- Defamation and free press
- Freedom of speech and expression
- Right to publish and circulate
- Right to receive information

- Right to conduct interviews
- Right to report court proceedings
- Right to advertise

However, there are certain restrictions in Article 19(2) to protect the nation and its integrity. The restrictions can be imposed in case of threats against:

Sovereignty and integrity of India

- Security of the State
- Friendly relations with foreign states
- Public order, decency or morality
- Contempt of court
- Defamation
- Incitement to an offence

Why is Freedom of the Press Important in India?

Free exchange of ideas: The press inspires people to think beyond the social norms and gives a platform to exchange ideas and thoughts that deserve to be heard by people all around the nation.

Holding the person or body accountable for their actions: Often, people try to cover up their actions and settle a case without bringing the media into it. The press brings to light such situations and makes sure that justice is served correctly with the backing of the common people.

Voice of the people: The press acts as a channel which writes and speaks the thoughts of the majority of people. It focuses on the issues that are suppressed and brings forward the ones that should be talked about.

Fourth pillar of democracy: Since the media is an independent body that challenges the Government, it can be referred to as the fourth pillar of democracy alongside the judiciary, legislative and executive bodies of the Government.

What is the Current State of the Press?

Although there has been some progress from the time when 'freedom of the media' can be estimated, the situation today is not very good. There have been lots of

cases of hate crimes, false accusations, trials due to wrongful portrayal, fake news, etc., in the recent years.

Let's take a look at the following:

- Fake News: We have all fallen victim to fake news which is so widely circulated that we believe it to be the truth.
- Paid News: Due to journalism and news-reporting being a low-paying job, some professionals often publish false news in exchange of a payment.
- Biased Media: High-paying criminals and politicians often pay media companies to cover 'good' and charitable moments of themselves. This leaves the audience biased, especially when it comes to elections.
- Crimes against journalists.

Regulation of the Press

The press in India is mostly self-regulating. The notion of self-regulation is that the media should be regulated by the press professional themselves. It means the media develops or creates a self-regulation mechanism independent from government control. They set out appropriate standards and codes of behaviour for the press to uphold their freedom of speech while monitoring and holding them accountable. The Media Self-Regulation Guidebook, Organization for Security and Co-operation in Europe, defines media self-regulation as "a joint endeavour by media professionals to set up voluntary editorial guidelines and abide by them in a learning process open to the public. By doing so, the independent media accept their share of responsibility for the quality of public discourse in the nation, while fully preserving their editorial autonomy in shaping it."

Current Regulation Mechanism of the Press

While the press in India follows self-regulation, there exist statutory bodies for the regulation of the press by issuing standards that take the role of guidelines. These bodies aim to achieve a balance between the aspects of public interest and solving the issue of accountability of the press. During the 1975 emergency, the encroachment made by the government shook the foundation of democracy and gagged the press. Post the emergency period, self-regulation was adopted by restoring the Press Council of India (PCI) under the Press Council Act 1978. This statutory body was established "for

the purpose of preserving the freedom of the Press and of maintaining and improving the standards of newspapers and news agencies in India.”

The main functions of the PCI are –

- Helping newspapers maintain their independence.
- Build a code of conduct for journalists and news agencies
- Help maintain “high standards of public taste” and foster responsibility among citizens
- Review developments likely to restrict the flow of news.

The PCI has the power to receive and enquire into the complaints concerning ethical violations and professional misconduct. It has the power to summon witnesses and take evidence under oath, demand copies of public records to be submitted, even issue warnings, and so on. The decisions of the PCI cannot be appealed before a court and are considered final.

However, the PCI has been severely criticized for being toothless due to the restrictions on its power. The PCI does not have the power to penalize the press for violation of the guidelines imposed by it. This means that though the press must follow these guidelines, there is no downside for them to not abide by them. This makes the enforcement of the guidelines difficult. Additionally, the PCI is also restricted in its jurisdiction as it enforces standards upon print media and cannot review electronic media like television and internet media.

As the PCI governs the print media, the Central Board of Film Certification (CBFC) governs all content screened in theatres or broadcasted via television. However, the CBFC does not have the power to issue guidelines concerning standards of news and journalistic conduct. In addition to short films and documentaries, news channels are an important part of the media. They are governed by the News Broadcasters Association (NBA), which can warn, censure, and impose fines for the violation of the Code of Ethics. However, they lack the statutory power required to ensure the proper implementation of such guidelines and codes. This brings the need for proper self-regulation mechanisms that rightly balance the freedom of the press and their social responsibilities towards the people.

2.6 HATE SPEECH AND CENSORSHIP IN INDIA

Definition Hate Speech and Scope

Hate speech is any communication that attacks or denigrates a person or group on the basis of attributes such as race, religion, caste, gender, sexual orientation, or disability. It can be expressed through spoken or written words, symbols, or gestures. Hate speech can have a devastating impact on individuals and communities, leading to violence, discrimination, and social exclusion.

Legal Framework

India has several laws that address hate speech, including:

Section 153A of the Indian Penal Code (IPC): Prohibits promoting enmity between different religious, racial, language, or caste groups. Section 505 of the IPC: Prohibits statements that incite violence or hatred against any person or group. The Information Technology Act (IT Act): Provides for the removal of online content that is deemed offensive, harassing, or defamatory.

Despite these laws, hate speech remains a significant problem in India. The definition of hate speech is often vague, and enforcement is inconsistent. This has led to concerns about the potential for arbitrary enforcement and the suppression of legitimate dissent.

Censorship Definition and Scope

Censorship is the suppression of speech or other forms of expression. It can be carried out by governments, organizations, or individuals. Censorship can take various forms, including:

Blocking access to information: This can be done through physical means, such as banning books or films, or through technological means, such as internet censorship.

Removing or altering content: This can be done by removing content from websites or social media platforms, or by altering the content itself.

Restricting or prohibiting communication: This can be done by restricting access to certain types of communication, such as through surveillance or by limiting the use of certain technologies.

Justifications for Censorship

Censorship is often justified on the grounds of protecting public order, morality, or national security. However, critics argue that censorship can be used to suppress legitimate dissent, protect the interests of the powerful, and limit the free flow of information.

Impact of Censorship

Censorship can have a significant impact on society. It can:

Limit access to information: This can hinder informed decision-making and prevent individuals from holding their government accountable.

Suppress dissent: This can stifle public debate and prevent the expression of minority views.

Undermine freedom of expression: This is a fundamental human right that is essential for a healthy democracy.

Balancing Free Speech and Censorship

Striking a balance between free speech and censorship is a complex task. There are legitimate reasons to restrict certain types of speech, such as incitement to violence or hate speech. However, it is important to ensure that censorship is not used to suppress legitimate dissent or limit the free flow of information.

The Role of Civil Society

Civil society organizations play a crucial role in addressing hate speech and censorship in India. These organizations can:

- Monitor and report on cases of hate speech and censorship.
- Advocate for legal reforms to protect freedom of expression and prevent hate speech.
- Educate the public about the dangers of hate speech and censorship.
- Promote tolerance and understanding among different groups in society.

2.7 INTERNATIONAL INSTRUMENTS ON FREE SPEECH AND EXPRESSION.

Several international instruments establish and protect the right to freedom of expression. These instruments, adopted by the United Nations and regional organizations, provide a framework for upholding this fundamental human right.

Universal Declaration of Human Rights (UDHR)

The UDHR, adopted in 1948, is a cornerstone of international human rights law. Article 19 enshrines the right to freedom of opinion and expression, stating that "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."

International Covenant on Civil and Political Rights (ICCPR)

The ICCPR, adopted in 1966, expands upon the right to freedom of expression in Article 19. It clarifies that this right includes the freedom to seek, receive, and impart information and ideas of all kinds, regardless of the form of expression or the means of dissemination.

Regional Instruments

In addition to these universal instruments, regional organizations have also adopted treaties and declarations that protect freedom of expression. These include:

European Convention on Human Rights (ECHR): Article 10 of the ECHR safeguards the right to freedom of expression, including the freedom to hold opinions and to receive and impart information and ideas without interference by public authority.

American Convention on Human Rights (ACHR): Article 13 of the ACHR guarantees the right to freedom of expression and the right to information.

African Charter on Human and Peoples' Rights (AfCHPR): Article 9 of the AfCHPR protects the right to freedom of expression, recognizing the freedom to seek, receive, and impart information and ideas of all kinds.

International Standards and Guidelines

Beyond these treaties, international organizations have developed standards and guidelines to promote and protect freedom of expression. These include:

UNESCO Declaration of Principles on Freedom of Expression and Information: This declaration outlines fundamental principles for upholding freedom of expression, including the right to seek, receive, and impart information and ideas.

OSCE Declaration on Freedom of Expression: This declaration reaffirms the commitment of OSCE participating States to protect freedom of expression and to promote media pluralism and independence.

Enforcing the Right to Freedom of Expression

While these instruments provide a strong legal framework for protecting freedom of expression, enforcement remains a challenge. Governments, civil society organizations, and individuals all play a role in upholding this right. Governments must ensure that their laws and policies comply with international standards and refrain from unjustified restrictions on freedom of expression. Civil society organizations can monitor and report on violations of freedom of expression, advocate for legal reforms, and provide legal assistance to those whose rights have been violated. Individuals can exercise their right to freedom of expression responsibly and engage in informed and respectful dialogue.

International instruments, regional conventions, and international standards provide a comprehensive framework for upholding freedom of expression. The right to seek, receive, and impart information and ideas are essential for a healthy democracy, informed decision-making and individual self-expression. Enforcing this fundamental right requires a concerted effort from governments, civil society, and individuals.

2.8 SOCIAL MEDIA AS AN ALTERNATE

Social media platforms have emerged as powerful alternatives to traditional media in many aspects, including news dissemination, information sharing, and public discourse. While traditional media outlets, such as newspapers, television, and radio, have long dominated the media landscape, social media has introduced a new dynamic, offering a more direct, interactive, and democratized approach to communication.

News Dissemination and Information Sharing

Social media has revolutionized the way news is disseminated and consumed. Traditional media relied on gatekeepers, such as editors and producers, to select and distribute news stories. In contrast, social media empowers individuals to share news and information instantly, bypassing traditional gatekeepers and enabling a more decentralized flow of information.

This shift has brought about several changes in the news landscape:

- **Real-time News Coverage:** Social media platforms allow for real-time coverage of events, providing breaking news updates and live streams as they happen.
- **User-Generated Content:** Social media enables users to share their own perspectives and experiences, contributing to a broader and more diverse range of news sources.
- **Global Reach:** Social media transcends geographical boundaries, allowing news to reach a global audience with unprecedented speed and reach.

Public Discourse and Civic Engagement

Social media has also transformed public discourse and civic engagement. Traditional media often served as one-way communication channels, where messages were broadcast from media institutions to the audience. In contrast, social media fosters two-way communication and enables direct interaction between individuals, organizations, and public figures.

This shift has facilitated:

- **Public Participation:** Social media allows individuals to participate in public discussions, share their opinions, and engage with policymakers and influencers.
- **Social Movements:** Social media has played a crucial role in organizing and mobilizing social movements, providing a platform for activism and collective action.
- **Democratization of Discourse:** Social media has democratized public discourse, giving a voice to marginalized groups and underrepresented perspectives.

Challenges and Limitations

Despite its transformative impact, social media also presents challenges and limitations. These include:

- **Misinformation and Disinformation:** The rapid and unfiltered nature of social media can make it susceptible to the spread of misinformation and disinformation.
- **Echo Chambers and Polarization:** Social media algorithms can create echo chambers, reinforcing existing beliefs and limiting exposure to diverse viewpoints.
- **Online Abuse and Harassment:** Social media can be a breeding ground for online abuse and harassment, particularly for marginalized groups and individuals.

Social media has emerged as a powerful alternative to traditional media, offering a more direct, interactive, and democratized approach to communication. While challenges remain, such as misinformation and online abuse, social media has transformed the media landscape, empowering individuals, facilitating public discourse, and enabling real-time news dissemination. As social media continues to evolve, its impact on society and democracy will continue to unfold.

2.9 CENSORSHIP IN SOCIAL MEDIA

Censorship in social media is the removal or suppression of content that is deemed to be harmful, offensive, or illegal. This can be done by the social media platform itself, or by governments or other third parties.

Reasons for Censorship

There are a number of reasons why social media platforms censor content. Some of the most common reasons include:

- To protect users from harmful content, such as hate speech, violence, and pornography.
- To comply with laws and regulations in different countries.
- To maintain a positive and welcoming user experience.
- To protect the platform's reputation.

Types of Censorship

There are a number of different types of censorship in social media. Some of the most common types include:

- **Blocking:** This is when a social media platform prevents a user or piece of content from being seen by other users.
- **Removing:** This is when a social media platform deletes a user or piece of content from the platform.
- **Demonetization:** This is when a social media platform removes advertising from a user or piece of content.
- **Shadow banning:** This is when a social media platform reduces the visibility of a user or piece of content without the user's knowledge.

Criticisms of Censorship

Censorship in social media is a controversial topic. Critics argue that it violates the right to free speech and can stifle important debate. They also argue that it is often ineffective and can be easily circumvented.

Supporters of Censorship

Supporters of censorship argue that it is necessary to protect users from harm and to maintain a positive and welcoming user experience. They also argue that it is important to comply with laws and regulations in different countries.

The future of Censorship in Social Media

The future of censorship in social media is uncertain. It is likely that social media platforms will continue to experiment with different types of censorship in an attempt to balance the need to protect users with the need to protect free speech.

Examples of Censorship in Social Media

There are many examples of censorship in social media. Some of the most well-known examples include:

- The removal of Donald Trump's account from Twitter and Face book following the 2021 U.S. Capitol riot.
- The blocking of content that is critical of the Chinese government on Weibo and WeChat.
- The removal of nipples from photos on Instagram.

- Censorship in social media is a complex issue with no easy answers. It is important to consider all of the different perspectives on this issue before forming an opinion.

2.10 PRIVATIZATION OF NEWS REGULATION

The privatization of news regulation refers to the shift from government-led regulation of the news industry to regulation by private entities or self-regulatory organizations. This can take various forms, including:

- Self-regulation: News organizations or industry bodies establish their own codes of conduct and ethical standards, and enforce them through peer pressure or internal disciplinary processes.
- Co-regulation: Governments and news organizations collaborate in setting standards and enforcing them, with the government providing oversight or acting as a backstop in cases of non-compliance.
- Privatized regulation: Governments delegate regulatory authority to private entities, such as independent regulatory boards or specialized agencies.

Proponents of privatized news regulation argue that it can lead to more efficient, effective, and flexible regulation, as private regulators are not bound by bureaucratic constraints and can adapt more quickly to changing media landscapes. They also argue that it can reduce government interference in the news industry and promote greater media freedom.

Critics of privatized news regulation argue that it can lead to conflicts of interest, as private regulators may be influenced by the commercial interests of the news organizations they regulate. They also argue that it can reduce transparency and accountability, as private regulators may be less subject to public scrutiny than government agencies.

The privatization of news regulation has been implemented to varying degrees in different countries. In some countries, such as the United Kingdom, there has been a significant shift towards self-regulation and co-regulation. In other countries, such as France, the government retains a more active role in news regulation.

The effectiveness of privatized news regulation is still being debated. Some studies have found that self-regulation and co-regulation can be effective in upholding

standards and reducing harmful content, while others have found that they can be less effective than government regulation.

Here are some examples of privatized news regulation:

- The Press Complaints Commission (PCC) in the United Kingdom: The PCC is an independent self-regulatory body that investigates complaints against newspapers and magazines. It has the power to issue public apologies, corrections, and fines.
- The Australian Communications and Media Authority (ACMA): The ACMA is a government agency that regulates the media industry in Australia. It has some regulatory powers over news organizations, but it also works collaboratively with the industry to develop and enforce codes of conduct.
- The Broadcasting Standards Authority (BSA) in New Zealand: The BSA is an independent self-regulatory body that oversees broadcasting standards in New Zealand. It has the power to investigate complaints against broadcasters and issue penalties.

The privatization of news regulation is a complex issue with no easy answers. It is important to weigh the potential benefits and drawbacks of different approaches to regulation before making a decision about how to regulate the news industry.

2.11 SOCIAL MEDIA COMPANIES PLATFORMS OR PUBLISHERS.

Social media companies can be classified as either platforms or publishers depending on how they define their role and responsibilities.

Platforms

A platform is a neutral intermediary that provides tools and infrastructure for others to create and share content. Social media platforms like Facebook, Twitter, and YouTube fall into this category. They provide the space and tools for users to create and share their own content, but they do not curate or control this content.

Under the platform model, social media companies are not legally liable for the content that users post on their platforms. This is because they are not considered to be publishers of the content. Instead, they are considered to be distributors of the content, which means that they are not responsible for the accuracy or legality of the content.

Publishers

A publisher is a company that selects, edits, and distributes content. Traditional publishers like newspapers and magazines fall into this category. They are responsible for the content that they publish, and they can be held legally liable for this content.

Social media companies can also act as publishers in some cases. For example, if a social media company curates or edits content before it is published, then it may be considered to be a publisher of the content. Additionally, if a social media company promotes or amplifies certain content, then it may also be considered to be a publisher of the content.

Hybrid Model

In reality, many social media companies operate under a hybrid model, where they act as both platforms and publishers. For example, a social media company may provide the tools and infrastructure for users to create and share their own content, but it may also curate or edit this content before it is published.

The hybrid model can be problematic because it can blur the lines between platforms and publishers. This can make it difficult to determine when social media companies are legally liable for the content that users post on their platforms.

Implications

The classification of social media companies as platforms or publishers has significant implications for their legal liability, their ability to moderate content, and their freedom of speech.

- **Legal liability:** If social media companies are classified as platforms, then they are generally not liable for the content that users post on their platforms. However, if they are classified as publishers, then they may be liable for this content.
- **Content moderation:** Platforms have more latitude to moderate content than publishers. This is because they are not considered to be responsible for the content that they remove. However, publishers have a greater responsibility to ensure that the content they publish is accurate and legal.
- **Freedom of speech:** Platforms are generally considered to have a greater right to free speech than publishers. This is because they are considered to be neutral

intermediaries that provide a space for others to express their views. However, publishers may have a greater responsibility to protect the freedom of speech of their users.

The debate over whether social media companies are platforms or publishers is likely to continue as the role of social media in society evolves.

2.12 SHADOW BANNING

Shadow banning, in social media and discussion forums, is the administrative practice of making a particular user's posts visible only to that user. Instead of notifying a user that his or her user generated content (UGC) has been blocked, the administrator simply prevents anyone else from viewing the user's content.

Shadow banning, also known as stealth banning, ghost banning, or comment ghosting, is a practice used by social media platforms to restrict or block a user's content from being seen by other users without the user being notified. This is typically done as a consequence of violating a platform's community guidelines or terms of service.

The goal of shadow banning is to encourage an undesirable contributor, such as a spammer or cryptojacker, to leave a group voluntarily because no one is interacting with their posts. The usual practice is for a moderator to notify a user that their contributions will no longer be accepted, but because the offender can still re-register under another user name, some administrators prefer to shadow ban offending contributors instead of outright banning them. To the offender, who is able to see his or her own posts, everything seems to be working as it should be. To everyone else in the online community, the offender becomes invisible.

Shadow banning is controversial because it allows an administrator or moderator to effectively become a censor and prevent specific users from interacting with other members of an online community on an equal basis. In January 2018, Project Veritas (PV) accused Twitter of systematically censoring certain individual's tweets by making their posts visible to the user's followers, but no one else. Instagram has also been accused of shadow banning members by using biased algorithms and not including certain hashtags in search.

2.13 ALGORITHMIC DOWNGRADING IN RECOMMENDER SYSTEMS.

Algorithmic downgrading in recommender systems refers to the intentional reduction of the visibility or ranking of certain items or content within a recommendation algorithm. This practice can be employed for various reasons, including:

- **Promoting Fairness and Diversity:** Algorithmic downgrading can be used to address potential biases or imbalances in recommendation systems. For instance, it can be used to prevent the overrepresentation of certain types of content or to ensure that a diverse range of items are recommended to users.
- **Enhancing User Experience:** Downgrading can be used to improve the overall user experience by filtering out irrelevant, low-quality, or misleading content. This can help users find the information or content they are most interested in more efficiently and effectively.
- **Adherence to Policies and Guidelines:** Algorithmic downgrading can be implemented to comply with specific policies, guidelines, or legal requirements. For example, it can be used to filter out content that violates terms of service, copyright laws, or other restrictions.
- **Protecting User Safety:** Downgrading can be used to protect users from potentially harmful or offensive content. This may include filtering out content that promotes violence, hate speech, or other harmful ideologies.
- **Content Moderation:** Algorithmic downgrading can be used as a form of content moderation, allowing platform owners to control the type of content that is visible to users. This can be used to maintain a desired brand image or community standards.

However, algorithmic downgrading also raises concerns about transparency and accountability. Users may not be aware of when or why their content has been downgraded, and it can be difficult to challenge or appeal these decisions. Additionally, algorithmic downgrading can have unintended consequences, potentially suppressing legitimate content or reinforcing existing biases.

To address these concerns, it is important for recommender system designers and operators to:

- Provide transparency: Clearly communicate to users when and why algorithmic downgrading is being applied.
- Establish clear guidelines: Define and publish clear guidelines for determining when and how algorithmic downgrading will be used.
- Implement effective appeal mechanisms: Provide users with mechanisms to challenge or appeal algorithmic downgrading decisions.
- Continuously monitor and evaluate: Regularly monitor the impact of algorithmic downgrading and evaluate its effectiveness in achieving its intended goals.
- Promote responsible AI practices: Adhere to responsible AI principles to ensure fairness, transparency, and accountability in the use of algorithmic downgrading.

Check your Progress

1. The ----- acts as a channel which writes and speaks the thoughts of the majority of people.
2. ----- is when a social media platform reduces the visibility of a user or piece of content without the user's knowledge.
3. Social media companies operate under a -----.
4. Social media transcends geographical boundaries -----

Glossary

- **User-Generated Content:** Social media enables users to share their own perspectives and experiences, contributing to a broader and more diverse range of news sources.
- **Democratization of Discourse:** Social media has democratized public discourse, giving a voice to marginalized groups and underrepresented perspectives.
- **Online Abuse and Harassment:** Social media can be a breeding ground for online abuse and harassment, particularly for marginalized groups and individuals.
- **Content moderation:** Platforms have more latitude to moderate content than publishers. This is because they are not considered to be responsible for the content that they remove. However, publishers have a greater responsibility to ensure that the content they publish is accurate and legal.

Answer to Check your Answer

1. Press
2. Shadow banning
3. Hybrid model
4. Global reach

Suggested Readings

<https://www.open.edu/openlearn/mod/oucontent/view.php?printable=1&id=1747>

<https://www.cambridge.org/core/journals/pmla/article/abs/platform-or-publisher/C59144B77FC9FDD8674E3CB8C1675309>

<https://ro.ecu.edu.au/cgi/viewcontent.cgi?article=7853&context=ecuworks3>

UNIT – 3

MEDIA – RELATED ACTS AND REGULATIONS**Overview**

- 3.1 Press And Registration of Books Act 1867
- 3.2 Registration of Newspapers
- 3.3 The Working Journalist Act
- 3.4 Press Council of India
- 3.5 Cinematograph Act
- 3.6 Official Secrets Act
- 3.7 Journalistic Defenses
- 3.8 Obscenity and Pornography
- 3.9 Constitution of the Censor Board
- 3.10 What is the meaning of Parliamentary Privileges?
- 3.11 Defamation
- 3.12 Contempt of Court
- 3.13 Landmark Cases related to Media
- 3.14 Cases relating to freedom of expression
- 3.15 Cases related to Press Content Regulation in Broadcast News
- 3.16 Cases related to government agencies
- 3.17 Cases related to Trade Association I India
- 3.18 Institutions related to media monitoring and regulations
- 3.19 Cases related to the Ministry of Information and Broadcasting (MIB)
- 3.20 Cases related to PrasarBharati
- 3.21 The Landmark cases related to TRAI
- 3.22 Case related to Indian News paper society
- 3.23 Case related to Broadcast Audience Research Council India (BARC)

Check your Progress

Glossary

Answer to check your progress

Suggested Readings

3.1 PRESS AND REGISTRATION OF BOOKS ACT 1867

An Act for the regulation of Printing-presses and newspapers, for the printed in India, and for the registration of such books and newspapers.

During colonial times, people wanted to free India from foreign rule and used newspapers to stir the spirit of nationalism in its people and make them aware of atrocities perpetrated by Britishers. The press and publishing industry regulations helped the government curb this resistance.

Since India's independence, certain modifications have been made to the laws concerning printing and publishing. However, these alterations have primarily pertained to particular situations, and a comprehensive review of the entire law is yet to be conducted to determine its alignment with contemporary times.

Reasons for Passing the Press and Registration of Books Act

The Act was enacted in 1867 during British India. According to this Act, the printer of the book must provide a complimentary copy of the book to the relevant state government and one or more copies to the Central Government. The primary motive for enacting this Act was maintaining a record of the books circulated in India. Each state government was obligated to compile a comprehensive catalogue of books, including essential bibliographic details. This catalogue encompassing all listed books had to be published at the end of every quarter, facilitating libraries to acquire complimentary copies of books and sustaining an uninterrupted record of all printed material in the nation.

Objectives of the Press and Registration of Books Act

The Press and Registration of Books was implemented with the sole aim of detailing the nature of the publications in British India. The Act aided in controlling the press and preventing incidents such as the Sepoy Mutiny and the Revolt of 1857.

The Act is not prohibitory, that is, it neither prohibits the functioning of the printing presses nor establishes any governmental control over the freedom of presses. However, the Act was a regulatory law that enabled the government to regulate printing presses and newspapers by a registration system and preserve copies of books and other matters printed in India.

As provided by the Preamble, the Act regulates printing presses and newspapers. Furthermore, the Act involves preserving and registering copies of newspapers and books printed in India.

The other common objectives of the Press and Registration of the Books Act are as follows:

- Protecting the information related to the printing establishments and their publications.
- Regulating the printing press and newspapers.
- Maintaining and registering copies of every book and newspaper printed in India.
- Preventing the publication of anonymous literature

Provisions of the Press and Registration of the Books Act

Rules Regarding Printing of Books and Newspapers

The Press and Registration of Books Act entails specific provisions regarding printing books and newspapers that every press in India must adhere to. The mentioned rules are as follows:

- Section 3 of the Act states how a book or paper will be printed in India. Per the statute, every book and paper should be printed legibly, highlighting the printer's name and the printing place. If such a book or paper is published, then the name of the publisher and the place of publishing shall be mentioned.
- Section 4 states that no person shall keep any printing press in its possession without prior approval in India.
- Section 5 details the rules regarding the publication of newspapers. All newspapers must be published in the manner provided in this section. The newspaper must have the name of the owner and editor of the newspaper along with the date of publication.

The newspaper's printer or publisher must be present (either in person or through an authorised agent) before the Presidency, District, or Sub-Divisional Magistrate within the local limits of the jurisdiction where the newspaper is printed. Therefore,

before publishing a newspaper or book, such a publisher/printer or an authorised agent shall declare that they are the actual printer/publisher of the book.

- Section 6 states the authentication of the declaration by the concerned judicial magistrate. The declaration shall be authenticated by the signature or seal of the concerned magistrate having jurisdiction.

There shall be two original copies of the declaration—one shall be deposited to the Magistrate’s Record and the other to the records of the High Court of competent Judicature.

- Inspection of the original declaration: The officer in charge of the original declaration may allow for the inspection after the payment of the required fee (one rupee) and permit applying for a copy of such declaration. (According to section-6)
- Section 7 provides that the copy of the declaration kept at the office bearing the court’s seal shall be prima facie evidence for proving the editor’s or publisher’s title.

Penalties Under the Press And Registration of the Books Act

Part IV of the Press and Registration of Books Act includes the penalty for an offence under the Act. The followings are the offences and their penalties as mentioned under the Act:

Offences	Section	Punishment
Any person who prints or publishes any book in contravention of the provisions of Section 3	12	The accused shall be convicted by a Magistrate with simple imprisonment for a maximum term 6 months or a maximum fine of Rs 2000 or both.
Any person keeps any press in his/her possession without authority and in contravention of Section 4	13	
Any person, regardless of whether in its declaration or in any other statement, gives any false statement before any competent Magistrate	14	

Any person prints, edits, or publishes, or cause to be printed, published, or edited, any newspaper knowing that it is in contravention with some provisions.	15	
Any person who has ceased to be a printer or publisher of any newspaper fails/neglects to make a declaration in compliance with Section 8.	15A.	The accused be convicted before a Magistrate and be punishable by a maximum fine of Rs 200.
If any printer of any book neglects to deliver copies of the same to the Government in accordance with Section 9.	16	
Negligence on the part of a printer of any newspaper published in India to deliver copies of the same per Section 11A to the Government.	16A	The accused be convicted before a Magistrate and punishable by a fine not exceeding Rs 50.
Failure on the part of the printer of any newspaper published in India to deliver its documents to the Press Registrar per Section 11B	16B	
If any person engages in connection with the collection of information under this Act, but he/she wilfully discloses any information or the contents of any confidential information.	19L	The accused shall be convicted by a Magistrate with simple Imprisonment for a maximum term of 6 months or a fine, which may extend to Rs 1000 or both.

Registration of Books

Section 18 of the Press and Registration of Books Act provides the registration of the memoranda of the books. A book is to be kept at every such office and by an officer appointed by the State Government; such a book is to be known as the Catalogue of Books printed in India.

Such memoranda of the book shall contain the following details:

- The name of the book and the contents of the title page
- The name of the author, editor, or translator of the book
- The language used in the book

- The subject and size of the book
- The name or firm of the printing press and the name or firm of the publisher
- The place of printing and publication
- Date of issuance of the book or newspaper from the media or the publication
- The first, second, or other number of the edition
- The number of sheets, leaves, or pages
- The number of copies of which the edition consists
- The price at which the book is sold to the public
- Whether the book is printed, cyclostyled, or lithographed
- The name and address of the proprietor of the copyright.

Such memoranda of books shall be published in the official gazette of India as per Section 19 of the Act.

3.2 REGISTRATION OF NEWSPAPERS

According to Sections 19A and 19B of the Act, the Central Government has the authority to appoint the Registrar of Newspapers in India to function all the powers conferred under the Act.

A Register of Newspaper is to be harboured by the Press Registrar and should consist of details which include the following

- Title of the newspaper,
- Place of printing,
- Language in which the newspaper is published,
- Number of days of publication in a year,
- Name of the editor,
- Printer and the publisher,
- The average number of copies printed,
- The retail selling price of each document,
- Periodicity of publication of the newspaper,

- Name and address of the owner of the newspaper and any other details, if required

Power of State and Central Government in Making Rules

Section 20 of the Press and Registration of Books Act empowers the State government to make necessary rules.

Section 20A empowers the Central Government to make rules, which include the following:

- Prescribing the particulars of a declaration
- Providing the form and manner in which the name of the editor, printer, and publisher is to be printed on the book or the newspaper
- Prescribing a way in which a register of newspapers is to be maintained,
- Prescribing the fees for furnishing copies of the extracts from the register,
- Prescribing a form in which the Press Registrar will prepare an annual report, etc.

The Press and Registration of Books Act is a pivotal move in regulating the printing industry and safeguarding freedom of expression. The Act ensures maintaining authenticity and credibility by maintaining social harmony. To maintain discrepancy and prevent the dissemination of false content, the Act requires the publishers to keep a record of their activity. Thus, an adequate track of ethical standards is ensured so that the public may have accurate and reliable content.

Thus, the Press and Registration of Books Act 1867 is a stringent law that provides specific regulatory standards for various printing presses and newspaper publishers, thereby averting any abuse of the right of freedom of the press.

3.3 THE WORKING JOURNALISTS ACT

The Working Journalists Act, 1955 is an Act of the Parliament of India that regulates the working conditions of journalists in India. It was enacted on 1955-10-26.

The Act provides for the following:

Definition of a working journalist: A working journalist is defined as a person who is employed in the production of a newspaper on a regular basis and whose primary

duty is the collection or preparation of news, or the preparation of editorials, articles or features for publication in a newspaper.

Wages: The Act provides for the fixation of minimum wages for working journalists. The rates of wages are fixed by the Wage Board appointed by the Central Government.

Hours of work: The Act provides for a maximum working week of 144 hours for working journalists. Every working journalist is entitled to a weekly rest of not less than 24 hours.

Leave: The Act provides for leave facilities for working journalists, including earned leave, sick leave and casual leave.

Security of service: The Act provides for security of service for working journalists. A working journalist cannot be dismissed or retrenched without an order of the Wage Board.

Penalties: The Act provides for penalties for the breach of its provisions.

The Working Journalists Act, 1955 is an important piece of legislation that protects the rights and interests of working journalists in India. It has been instrumental in improving the working conditions of journalists in the country.

3.4 PRESS COUNCIL OF INDIA

Press Council Act, 1978 is an Act to establish a Press Council for the purpose of preserving the freedom of the press and of maintaining and improving the standards of newspaper and news agencies in India. It extends to the whole of India.

Under the Press Council Act, the Council by the name Press Council of India has been established 1st March 1979. The Council is a body corporate having perpetual succession. The Council consist of Chairman and 28 other members. Section 13 of the Press Council Acts lays down the objects and functions of the Council. The important functions of the Council are:

- To help newspaper and news agencies to maintain their independence
- To build up a code of conduct for newspapers, news agencies and journalists
- To keep under review any development likely to restrict supply and dissemination of news of public interest and importance

- To concern itself with the development such as concentration of or other aspects of ownership of newspapers and news agencies which may affect the independence of the press.

The Press Council Act empowers the Press Council to make observations in respect of conduct of any authority including Government, if considered necessary for performance of its functions under the Act. It can warn, admonish or censure the newspaper, the news agency, the editor or the journalist or disapprove the conduct of the editor or the journalist if it finds that a newspaper or a news agency has offended against the standards of journalistic ethics or public taste or that an editor or a working journalist has committed any professional misconduct. One year after emergency PCA came into act. The PCA was set up in 1966 under the Act of 1965 when Indira Gandhi was I&B Minister. It was aimed at preserving the freedom of the press & maintaining and improving the standards of newspapers and news agencies in India. It was established in 1975 after the proclamation of emergency. The government enacted a new PCI Act in 1978 and the new PCI came into Act in 1976. PCI consists of a chairman and 28 members. Chairman is usually a highly experienced judicial person, usually a former Supreme Court Judge. He is appointed by a committee headed by the Chairman of Rajya Sabha. --- 20 members are dominated by the panels submitted by working journalist bodies consisting editors and owners. Of these 13 are located from among the working journalists rest from Editors of language press owners, small earned media newspapers and news agencies. Five member of the parliament (2fromRajya Sabha and 3 from Lok Sabha) are also included. The term of the chairman is 3years. The term of the members which Is normally 3 years ends with the term of the council. The chairman can continue till the next council. The chairman can continue till the new council takes over but not beyond 6 months.

A retired member can be re-nominated only once 3 members can be nominated by UGC University if Bar and Council of India and Science Academy.

Press council does not deal with Electronic Media. It has quasi judicial function and has therefore been vested with the powers of the civil court i.e. it can summon and examine witnesses, documents, receivers evidence and affidavit issue commission for examining witnesses, documents or nay other, matter which may be prescribes. The

council holds open enquiries or complains received against newspapers, news agencies, journalists etc. on the basis of the enquiry the council declares its adjudication.

It has issued guidelines on some important matters like the riots, Jatt riots, communal tension and their reporters. The council has powers to levy a graded fee on newspapers and news agencies to meet its expenditure and to reduce its dependence and government financial support. - In times of absence of self regulation by newspaper industry the PCA steps in suo- moto complains received from quarters.

The council deals with professional and industrial aspects of newspapers editorial and circulation. The act defines what is a big newspaper, what is a medium newspaper and what is small newspaper.

A big newspaper means the newspaper which has a circulation exceeding 50,000 copies in all editions put together and the medium newspaper means minimum 15,000 copies and maximum 50,000 copies circulation. A small newspaper means a circulation not exceeding 15,000.

A common code in broadcasting was evolved in 1962 by the fourth Asian broadcaster's conference at Kuala Lumpur to which India was party. According to certain cardinal principle should be followed by broadcasters and television organizations these are;

- They should ensure the objectives presentation of news and fair unbiased content
- They should promote the advancement of agitation and culture.
- They should raise and maintain high standards of decency and decorum in all programmes.
- They should provide programmes for which by variety and content will inculcate the principles of good citizenship.
- They should come out with communal harmony and, religious tolerance, and international understanding. - They should treat controversial public issues in an impartial and dispassionate manner.

3.5 CINEMATOGRAPH ACT

The Cinematograph Act, 1952 (the Act), ensures that films fulfil the objectives prescribed by law. In the Act is a provision for the establishment of a Central Board of Film Certification (the Board). This is the regulatory body in India that issues a certificate to the makers of films for public exhibition. Once the Board has examined a film, the Board can:

- Sanction the film for unrestricted exhibition;
- Sanction the film for public exhibition limited to adults;
- Direct such modifications and excisions in the film before sanctioning the film to any of the above;
- Refuse to sanction the film for exhibition completely.

One of the first cases where the issue of censorship of film was raised is *K. A. Abbas vs Union of India*, where the Supreme Court of India considered the vital question related to pre-censorship of cinematography in relation to the freedom of speech and expression that is guaranteed under the Constitution of India. It was held by Hidayatullah, C.J, that censorship of films which includes pre-censorship was constitutionally lawful. Though, he added, that unjustified restriction on freedom of expression by the Board should not be exercised. In the case of *S. Rangrajan vs Jagjivan Ram*, Supreme Court faced a similar question, and was of the view that 'if the exhibition of the film could not be validly restricted under Article 19(2), risk of procession and demonstration was not a valid ground to suppress the same.' The Supreme Court added that it was the State's duty to protect the freedom of expression. The Supreme Court of India in giving its judgement in the case of *Bobby Art International vs Om Pal Singh Hoon* was of the opinion that, a film must be judged in its entirety. The court added that where the theme of the film is to condemn violence and degradation, scenes of expletives to advance the message, which was the main intention of the film, is permissible.

Types of Certifications

There are mainly four kinds of certifications given by the Central Board of Film Certification:

1. Universal (U): This type of certifications is the Unrestricted Public Exhibition, and the same holds no limitations for the age groups that may watch the same. They could be family, educational or social oriented themes. This category has fantasy violence and minimal foul language. When a movie is being certified U by the Board, it must ensure that the movie is suitable for a family to watch it together including the children.

2. Parental Guidance (UA): This type of certification explains that the film is appropriate for all age groups. However, it is in the interest of the children below the age of 12 to be accompanied by their parents. The reason could be that the theme of the movie may not be the most appropriate for the child without the guidance of their parents.

3. Adults Only (A): As the certification suggests, this type of film is restricted to adults only. Persons above the age of 18 are adults, for the meaning of this certification. The theme may contain disturbing, violent, drug abuse and other related scenes which are not considered suitable for viewing by children who may be influenced by the same negatively. Films that meet the requisites of the abovementioned criteria but are not suitable for exhibition to children or those below the age of 18 shall be certified A.

4. Restricted to Special Class of Persons (S): This is the last type of the certifications under the board, and the same explains that the films which are rated S are meant for a special class of persons only. For example, doctors. If the Board is of the opinion that with regards to content, nature and the theme of the film is to be restricted to members of a class of persons or any profession, the above certification shall be given to such film.

Objectives of Film Certification

1. The main objectives of the Board for the above are as follows:

1. To ensure that the medium of the film is responsible. Additionally, to safeguard the sensitivity of standards and value of the society.
2. To ensure that creative freedom and expression are not unjustifiably curbed.
3. To ensure to adapt to the social changes.
4. To ensure the theme of the film provides a healthy and clean entertainment.
5. To ensure that the film is of cinematically an adequate standard and aesthetic value.

2. In pursuance of the above, the Board must ensure that:

1. Activities that anti-social such as violence are not justified or glorified;
2. The way criminals are depicted, and other related words or visuals must not incite the commission of any kind of offence;
3. The scenes showing ridicule and abuse of mentally and physically handicapped, cruelty or abuse of animals, involving children as victims of violence and abuse must not be presented needlessly;
4. Avoidable or pointless scenes of cruelty, horror and violence that are intended to provide entertainment but may have the effect of dehumanizing or desensitizing people are not shown;
5. Scenes that glorify or justify drinking are not shown;
6. Scenes that tend to justify, glamorizes or encourage drug addiction are not shown. Additionally, similar scenes for the consumption of tobacco or smoking must not be shown;
7. Human susceptibilities are not offended by obscenity, vulgarity or obscenity;
8. Words with dual meanings that cater to dishonorable instincts are not used;
9. Scenes denigrating or degrading women in any manner is not shown;
10. Scenes that involve sexual violence against women in the form of rape or any other form of molestation are avoided. If the theme of the movie requires so, the same must shall be reduced to a minimum and no details are to be shown. The same goes for scenes that involve sexual perversion;
11. Words or visuals contemptuous of religious, racial or other groups must not be presented;
12. Words or visuals that promote obscurantist, communal, anti-national and anti-scientific attitude are not shown;
13. The integrity and sovereignty of the country is not called in question;
14. The security of the country is not endangered or jeopardized;
15. Relations with foreign states are not overwrought;
16. Public order is maintained, and not hindered;
17. Words or visuals involving defamation of a body or an individual, or contempt of court are not shown;
18. National emblems and symbols are not presented except according to the provisions of Emblems and Names (Prevention of Improper Use) Act, 1950 (12 of 1950).

3. The Board shall additionally ensure that a film:

1. Is judged as a whole from the perspective of its overall impact; and
 2. Is inspected in the light of the period illustrated in the film along with contemporary standards of India and the people who the movie is related to, to ensure that the film does not corrupt the morality and ethics of the audience.
- Applying to all of the above categories, the Board shall ensure the titles of each film is carefully scrutinized to ensure they are not vulgar, violating, provocative or offensive to the guidelines mentioned above.

Conclusion

In India, the basis on which a film is censored or banned has been evidently traditional norms. That being said, what is censored today, may not be censored tomorrow. The socio-economic dynamics of a country is continually evolving. Hence, all regulations must try to adapt to the same. The Constitution of India guarantees freedom of speech and expression with justifiable limitations on certain expressions like contempt of court, morality and decency, the security of the State, public order, incitement to an offence, defamation, etc. and rightly so.

3.6 OFFICIAL SECRETS ACT

What is 'Official Secret'?

It includes any kind of information; any official code, password, sketch, plan, model, article, note, document or information. The only qualification is that it should be "secret". The word "secret" or "official secrets" actually remain undefined in the Act.

The only clarity being that the Act applies only to official secrets and not to secrets of a private nature. Hence, the Act extends to ministry or department of the government, but not to an incorporated body like a university, government company or public corporation.

Since, there is no definition of "secret" in the Act the Government has the discretion to classify anything and everything as a "secret" as per the Official Secrets Act. The typical practice of the government is to treat any information as secret, merely because it may embarrass the government or the party in power.

The OSA 1923 was enacted with the purpose of protecting the safety and integrity of the State, but unfortunately the wide discretionary powers conferred upon the administrative authorities with a view to facilitating the task of protection of National Security were being exercised indiscriminately. There is no doubt that a statute of the nature of OSA is an indispensable requirement of a sovereign State but at the same time without necessary precaution, it is a grave threat to Freedom of the Press and transparency in governance.

The OSA and ARTICLE 19(1) (A):

Article 19(1) (a) of the Constitution guarantees the Right to Freedom of Speech and Expression to every citizen. The Freedom of Speech and Expression does include the right to acquire and disseminate information. The OSA 1923, it is claimed, violates all these rights by virtue of the restrictions it puts on the Freedom of Information. The vague provisions of the OSA 1923 also facilitate attempts on the part of the Government to threaten Media Personnel.

While discussing the conflict between these two Acts, it would be remarkable to quote the Judicial verdict in the famous State of UP v Raj Narain:

"In a government of responsibility like ours, where all the agents of the Public must be responsible for their conduct, there can be but few secrets. The people of this country have a right to know every public act, everything that is done in a public way, by their public functionaries. They are entitled to know the particulars of every public transaction in all its bearing. The right to know, which is derived from the concept of freedom of speech, though not absolute, is a factor, which should make one wary, when secrecy is claimed for transactions, which can, at any rate have no repercussions on public security."

Commission and Committee Reports on the Constitutionality of the OSA

Several Commissions and Committees have reviewed the OSA; the Press Laws Inquiry Committee (1948), the Press Commission (1954), the Law Commission (1971) and also by a Study Group appointed by the Central Government in 1977.

The First Press Commission though endorsed the Pro- Secrecy stance of the Press Laws Inquiry Committee did also make one other important observation:

"We agree with the contention that merely because a circular is marked secret or confidential, it should not attract the provisions of the Act, if the publication thereof is in the interest of the Public and no question of National Emergency and interest of the State as such arises."

The Second Press Commission and the Press Council of India had recommended that Section 5 be scrapped. The commission suggested its replacement by provisions modelled on those of the British Freedom of Information Bill, 1978. The Council asked for the repeal of the OSA and to enact a new legislation, which may be called Freedom of Information Act.

In the era of RTI this British Raj draconian Act is against the very spirit of transparency in governance in a modern democratic state like that of ours. Verappa Moily led 2nd Administrative Reforms Commission recommended this act to be repealed or scrapped. The Moily Commission has suggested that safeguards for State Security should be incorporated into the National Security Act (NSA) instead of the OSA.

3.7 JOURNALISTIC DEFENSES

The 'exceptions' discussed in the preceding paragraphs are very important. In addition to the defences available in cases already stated (private or civil wrong for which the wronged person may get redress in a law court) there are four special defences available to journalists in an action for defamation. They are:

1. Justification
2. Fair comment
3. Privilege
4. Apology ground for exception is 'good faith' and 'public interest'. Explain these two concepts briefly.

In an action for defamation the complainant has to first prove:

- 1) that the defamatory statement is published;
- 2) that it refers to him, and
- 3) that it is false.

Media Ethics and Laws The defendant in his defence can prove that

- 1) the statement does not bear defamatory meaning;
- 2) that it does not refer to the complainant or to any other person on behalf of
- 3) whom the complainant can initiate criminal proceedings under Cr.P.C.;
- 4) that the statement is privileged;
- 5) that the case is time-barred;
- 6) that the suit is barred by judicator.

These defences are available to any person making an imputation against the other. In addition to these, the special defences mentioned above are also available.

Justification

The defence that the statement is true is called the plea of justification. We have observed in the exception given in Sec. 499 IPC studied earlier, that truth of the imputation by itself is not sufficient in a criminal proceeding. Public good is also another ingredient that must have been involved. But in a civil suit, truth of the, defamatory statement is a complete defence. The burden of proof is on the defendant. If the impugned statement is provided to be substantially true it is enough. But if the plea of justification is taken in a criminal complaint, the evidence rendered should be such as would result in the conviction of the complainant for the alleged offence. The plea of justification is like the razor's edge, for if the defendant does not use improperly it may cause injury to him. If the defendant does not succeed in proving every material part of his statement, the very fact that he has taken the plea of justification, may be treated as aggravation of the offence and may result in the award of increased damages.

air Comment

Fair comment on a matter of public interest does not amount to libel. In a plea of fair comment three points arise:

- (i) The comment relates to a matter of public interest.
- (ii) It is only a comment and not a statement of fact.
- (iii) The comment is fair.

Any matter that affects the public at large is a matter of public interest. Conduct of persons in public office or sanitary conditions, public performances of dance, drama or publication of books or release of films for public exhibition etc., are all matters of

public interest. Everyone is entitled to comment on such matters. Comment, being a matter of opinion, is enough if it is fair and honest. Others may agree with the comment but the commentator is not called upon by the law to justify it. The comment or criticism is said to be fair if an ordinary set of men with ordinary judgement, would think so. Criticism should not be actuated by malice. It should be a reasonable inference from the facts, which must be truly stated. Privilege 'there are some occasions when a person will not incur the liability even if the reporter statement published is defamatory. Such immunity is conferred by law for protection of public interest. A defence founded on such immunity is called the 'privilege'. Privilege is of two kinds (i) Absolute Privilege (2) Qualified Privilege.

Absolute Privilege: On grounds of public policy no action is taken for publication of reports or statements, however false they may be in cases covered by absolute privilege. Reports of parliamentary proceedings and coverage of proceedings of state legislatures, are protected by Art. 361-A of the constitution itself. So no action can be taken for publishing statements made by members of either House of Parliament or legislature however damaging they may be to the interests of any person. But the report must be substantially true. This protection will not be available for publication of statements made by M.P.'s or M.L.A.'s outside Parliament or legislature, and also to the expunged portions of the proceedings of the House.

Qualified Privilege: Judges, counsels and parties in judicial proceedings are absolutely privileged and immune from liability for statements made even if they are defamatory. But newspaper reports of court proceedings come under qualified privilege in our country. Publication of statements relating to affairs of state and reports of public meetings are also given protection of qualified privilege. As far as reports of public meetings are concerned, care should be taken that (a) the meeting is lawful; (b) the proceedings relate to matters of public importance; and (c) the report is fair and accurate.

The defence of qualified privilege will not be available if the defendant is actuated by malice. Malice need not be express malice. It includes indirect or improper motive or any motive other than a sense of duty.

3.8 OBSCENITY AND PORNOGRAPHY

Obscenity

Legal definitions of obscenity vary from country to country and may change over time. In the United States, the Supreme Court has defined obscenity as material that meets the following three-pronged test:

It appeals to a prurient interest in sex.

It depicts sexual conduct in a patently offensive way. The lacks serious literary, artistic, political, or scientific value. Material that is obscene is not protected by the First Amendment. There are a number of exceptions to the prohibition on obscenity, such as material that is used for educational or medical purposes.

Pornography

Pornography is a broader term than obscenity and encompasses any material that is sexually explicit. Pornography is not necessarily illegal, but it may be considered to be obscene if it meets the three-pronged test. There are a number of concerns about the use of pornography, such as:

It can lead to addiction. It can contribute to violence against women. It can exploit children. Debate over obscenity and pornography The debate over obscenity and pornography is often framed in terms of freedom of speech versus the protection of society from harm. Proponents of free speech argue that adults should have the right to consume whatever material they choose, even if it is considered to be offensive or harmful. Opponents of pornography argue that it is harmful to individuals and to society as a whole. The best course of action may vary depending on the specific circumstances. The impact of obscenity and pornography on children. The role of the internet in the distribution of obscenity and pornography. The international dimensions of the debate over obscenity and pornography.

3.9 CONSTITUTION OF THE CENSOR BOARD

The Board consists of a Chairman and non-official members, all of whom are appointed by the Central Government. It is headquartered in Mumbai, Maharashtra. Additionally, it has nine Regional offices, namely, Chennai, Bangalore, Hyderabad, New Delhi, Guwahati, Cuttack, Kolkata and Thiruvananthapuram. Regional Offices, as

mentioned above, are assisted by the Advisory Panels. The Advisory Panels, like the Board, is selected by the Central government. The members chosen for the panel are from different walks of life, and they are chosen for a period of 2 years. It has a two-tier jury system, the Examining Committee and the Revising Committee.

Common Reasons for Censorship or Banning of a Film

In light of the history of why a film has been banned, or parts of it are censored, the main categories for why the same is done are as follows:

1. **Sexuality:** A rigid social structure has been followed in Indian society. Hence, a medium which portrays sexuality regardless of the audio, written or visual form, which has not been fathomed by the society and is concerned a social stigma is banned on the grounds that it might have the effect of undignified morals of Indians.
2. **Politics:** The isolation of political forces is not far when one talks about censorship. The description of an allegorical political scene, directly or indirectly, is banned by the authorized party to it. Overt political overtones are not appreciated by the government and hence is a common reason why certain films are either entirely banned, or such scenes are censored or removed.
3. **Communal Conflict:** Under a heterogeneous nation like India, if a film incites or spurs any type of communal conflict, the same is censored. The aim is to avoid the consequences such a film would have on the audience it intentionally or unintentionally targets. If the state believes that a movie would open a window for riots by a community for the way they have been portrayed in the film, the same is banned by the Board or censored.
4. **Incorrect Portrayal:** Sometimes, a situation arises where a well-known personality objects his own depiction in a medium which would be exhibited, and consequently goes for censoring the same. For more clarity, in a situation where the medium is of biographical nature, and the person on whom it is based does not approve the authenticity of the same, there have been times when the person has sued for the medium not to be released, or be edited and released upon approval of such person.
5. **Religion:** Religion does not appreciate any type of defiance or disobedience towards the values it proliferates. Hence, any medium which directly or indirectly distorts any aspect of the religion including its preaching, values, idols, to name a few, is highly criticized and therefore, censored.

6. Extreme Violence: Indubitably, the portrayal of extreme gore and violence may meddle and disturb the human mind. Viewing such scenes may have a negative psychological effect on the mind. If the Board of a similar opinion that such a scene through any medium may have an underlying negative impact on the viewer, contrary to the entertainment or knowledge such scene tries to bestow, the same may be banned, edited or censored by the Board in public interest.

3.10 WHAT IS THE MEANING OF PARLIAMENTARY PRIVILEGES?

- Parliamentary privileges are the rights and immunities enjoyed by members of Parliament (MPs) in India to enable them to discharge their duties and functions without interference or intimidation.
- Sources: These privileges are derived from the Constitution of India, parliamentary conventions, laws made by the Parliament, rules of Lok Sabha and Rajyasabha, and judicial interpretations.
- Constitutional Provisions: Parliamentary privileges are defined in Article 105 of the Indian Constitution. The members of Parliament are exempted from any civil or criminal liability for any statement made or act done in the course of their duties.
- Co-terminus with membership: The privileges are claimed only when the person is a member of the house. As soon as he ends to be a member, the privileges are said to be called off.
- These privileges are essential so that the proceedings and functions can be made in a disciplined and undisturbed manner.
- In India, the privileges of members of Parliament are specified in the Constitution, the Rules of Procedure and Conduct of Business in Lok Sabha, and the Rules of Procedure and Conduct of Business in Rajya Sabha.
- It is important to note that parliamentary privileges are not absolute and are subject to certain limits. For example, MPs are expected to use their privileges responsibly and not abuse them for personal gain.

How are the Parliamentary Privileges Classified?

- Parliamentary privileges are intended to protect the independence and integrity of the legislative process and to allow lawmakers to speak and act freely without fear of reprisal or legal consequences.

- **Individual Privileges:** Individual privileges refer to the rights and immunities enjoyed by members of the Indian Parliament and State Legislature to enable them to perform their duties without fear of interference or prosecution.
- **Collective Privileges:** Collective privileges in India refer to the rights and immunities that are enjoyed by both Houses of the Indian Parliament and State Legislature as a whole, as well as their members and officers.
- Members cannot be arrested during the session of Parliament 40 days before the beginning and 40 days after the end of a session.
- Members have freedom of speech in Parliament, and no member is liable to any proceedings in any court
- They are exempted from jury service when Parliament is in session.
- Right to publish its reports, debates, and proceedings.
- Right to exclude strangers from its proceedings
- Right to make rules to regulate its own procedure
- Right to punish members as well as outsiders for breach of its privileges
- The courts prohibited inquiring into the proceedings of a House.
- No person can be arrested without the permission of the presiding officer.
- Parliamentary privileges are an important aspect of the legislative process, as they help to ensure the independence and integrity of the legislative body. These privileges are intended to protect the ability of lawmakers to speak and act freely.
- By providing immunity from arrest and legal process, parliamentary privileges allow members of parliament to carry out their duties and responsibilities without fear of intimidation or interference.
- In addition, parliamentary privileges such as the privilege of confidentiality and the privilege of access allow members of parliament to obtain and share information that may be crucial to their decision-making processes.
- Overall, parliamentary privileges are an important part of the checks and balances that help to safeguard the independence and integrity of democratic institutions and ensure that they can function effectively.

What are the Challenges and Issues Pertaining to Parliamentary Privileges?

- There are several challenges associated with parliamentary privileges in India. Some of these challenges include

- **Scope of privileges:** One challenge is determining the scope and limits of parliamentary privileges. While these privileges are intended to protect the independence and integrity of the legislative process, they can also shield lawmakers from accountability and scrutiny.
- **Conflict with constitutional principles:** Parliamentary privileges may sometimes conflict with other constitutional principles, such as equality before the law. For example, the privilege of immunity from arrest and legal process may be seen as giving members of parliament special privileges that are not available to other citizens.
- **Misuse of privileges:** There have been instances where parliamentary privileges have been misused by lawmakers in India. For example, some lawmakers have used their freedom of speech privilege to make inflammatory or offensive comments or false or baseless allegations.
- **Lack of transparency:** The process for claiming and enforcing parliamentary privileges in India can be opaque and lacks transparency. This can make it difficult to hold lawmakers accountable for their actions and undermine public trust in the legislative process.
- **Inadequate oversight:** There is a lack of adequate oversight and mechanisms for enforcing parliamentary privileges in India. This can make it difficult to hold lawmakers accountable for abuses of these privileges and can lead to a lack of confidence in the legislative process.

How can Parliamentary Privileges be Used Effectively?

Parliamentary privileges are an important aspect of the legislative process, as they help to ensure the independence and integrity of the legislative body. To use these privileges appropriately, lawmakers should follow a few best practices:

1. **Use privileges responsibly:** Members of parliament should use their privileges responsibly and should not abuse them for personal or political gain. This means avoiding using privileges to make inflammatory or offensive comments or false or baseless allegations.

2. Respect the rights of others: Members of parliament should respect the rights of others and should not use their privileges to infringe on the rights of others. This includes avoiding using privileges to harass or intimidate others or to engage in discriminatory or exclusionary behavior.
3. Be transparent: Members of parliament should be transparent in their use of privileges and should be open and accountable for their actions. This means being open and honest about the reasons for claiming privileges and being willing to justify their use when necessary.
4. Follow parliamentary procedures: Members of parliament should follow established parliamentary procedures when claiming and enforcing privileges. This includes respecting the rules and standing orders regulating the procedure of Parliament, and adhering to the principles of impartiality and fairness.

Overall, by following these best practices, members of parliament can use their privileges appropriately and in a way that serves the best interests of the institution and the public. This can help to ensure that the legislative process is independent, transparent, and accountable and that it serves the needs and interests of the community.

3.11 DEFAMATION:

Defamation, in law, attacking another's reputation by a false publication (communication to a third party) tending to bring the person into disrepute. The concept is an elusive one and is limited in its varieties only by human inventiveness.

Defamation has been defined under Section 499 of the Indian Penal Code (IPC) as whoever, by words either spoken or intended to be read, or by signs or by visible representations, makes or publishes any imputation concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm, the reputation of such person is said to defame that person.

Libel and slander

Libel and slander are the legal subcategories of defamation. Generally speaking, libel is defamation in written words, pictures, or any other visual symbols in a print or electronic(online or Internet-based) medium. Slander is spoken defamation. Usually, liability for a defamation falls on everyone involved in its publication whose

participation relates to content. Thus, editors, managers, and even owners are responsible for libellous publications by their newspapers.

3.12 CONTEMPT OF COURT:

Contempt is nothing but lowering down prestige of the court. The objective of the contempt of court is basically to maintain the essence of respect towards court. Contempt is defined under section 2 of the contempt of courts Act 1971. The meaning of contempt is wilful disobedience to or open disrespect of a court or judge. Contempt means lack of respect or reverence for something.

Types of Contempt

- Civil
- Criminal

Civil contempt means wilful disobedience to any judgement, decree, direction, order, writ or other process of a court or wilful breach of an undertaking given to a court. Criminal Contempt means the publication (whether by words, spoken, written or by signs or by visible representations, or otherwise) of any matter or doing of any other act whatsoever which scandalizes, prejudices or interferes the administration of justice in any other manner.

- Exception to contempt
- Innocent Publications
- Fair Comments/ Criticism

Punishment:

Simple imprisonment upto six months and or fine. Where the contempt of court is committed by a company each person responsible for running that company will be liable for punishment.

Exemption:

If the accused apologizes to the satisfaction of the court, the person may be discharged or punishment may be remitted

3.13 LANDMARK CASES RELATED TO MEDIA.

What is a Media Trial?

Whenever there is any sensitive case that comes to be tried before the court, then among the people there is an anticipated upsurge in curiosity. Always looking forward to sensational news, Media including newspapers, television channels, news websites, etc. start publishing their own interpretation of facts. It is called investigative journalism and is not prohibited in India. The influence of media coverage via newspapers and television on an individual by creating a perception of innocence or guilt even before the Court of law announces its judgment, it is called as “Media Trial” or ” Trial by Media”.

In 1999, Jessica Lal (model turned barmaid) working in a restaurant owned by socialite Bona Ramani in Mehrauli, South Delhi’s, was shot dead by Manu Sharma (alias SiddharthVashisth), son of Congress former Union Minister, Venod Sharma after Jessica refused to serve liquor to him and his friends. This case immediately gained media coverage after the murder when the accused was acquitted by the trial court. This case became one of the top cases where the public pressure and media compelled the justice system to take a second look at this case. Though Manu Sharma was acquitted initially in the year 2006 as the Delhi police failed to sustain the grounds on which they had built up their case after public outcry due to the media coverage of the case, the Delhi High Court sentenced him to life imprisonment.

3.14 CASES RELATING TO FREEDOM OF EXPRESSION

R. Rajagopal vs State of Tamil Nadu

A prisoner named Auto Shankar, who was held for murder and was sentenced to life imprisonment and death sentence, wrote an autobiography when he was imprisoned. The book discussed his personal life and his relation with many senior police officials, lot of whom have said to be involved with him in many illegal acts. Before his death sentence, he handed over the book to his wife after informing the prison officials of the same and the wife gave the book to the petitioners i.e., the editor, the associate editor, the printer and the published of a Tamil Magazine, for its publication. The Inspector General, when he got to know about the book, wrote to the published stating that the contents of the book were false and untrue, and that the book was defamatory in nature and that strict legal action will be taken against them if they proceed with publishing

the book. The Tamil Magazine editor filed a petition against the Inspector General of Prisons to prevent him from violating their and the prisoner's right to freedom of speech and expression.

The Supreme Court in this case held that the magazine had the right to publish the autobiography written by the prisoner, without his consent or authorization. It held that the state cannot prevent the publication but may sue the plaintiff for defamation after the article is published, but they had no right to stop the petitioners from publishing the book. It held that every person has the right to publish his/her autobiography because of his/her fundamental rights under Article 19 of the Indian Constitution and hence, the case was in favour of the petitioners.

3.15 CASES RELATED TO PRESS CONTENT REGULATION IN BROADCAST NEWS

Some cases relating to press content regulation in broadcast news:

FCC v. Pacifica Foundation (1978): This landmark case involved the broadcast of a radio monologue that contained vulgar and profane language. The Supreme Court held that the FCC could not censor the broadcast, as it did not meet the FCC's standard of "indecenty." This case helped to establish the First Amendment protections for broadcast media.

TV Today Network Limited v. News Laundry Media Private Limited (2020): This Indian case involved a news program that criticized a television channel for its coverage of a controversial issue. The Supreme Court held that the news program was protected by the right to free speech, as it was a "fair comment" on a matter of public interest. This case helped to clarify the scope of the right to free speech in India.

TV Today Network Limited v. News Laundry Media Private Limited (2020) case

Sudarshan TV v. Union of India (2020): This Indian case involved a news channel that broadcast a program that was accused of promoting hatred against a particular religious' community. The Supreme Court held that the broadcast was illegal, as it violated the Indian Constitution's prohibition on hate speech. This case highlighted the importance of balancing the right to free speech with the need to protect vulnerable groups from discrimination.

These cases illustrate the complex and often contentious issues surrounding press content regulation in broadcast news. The courts must carefully balance the competing interests of free speech, public safety, and individual rights in order to ensure that broadcast news is both informative and responsible.

The Supreme Court, in a bid to tighten the reins on TV news channels, has demanded stronger regulations for media broadcasters. The court, led by Chief Justice D.Y.Chandrachud, emphasized the necessity of an enhanced self-regulatory mechanism. The court specifically mentioned some channels going "berserk" during their coverage of actor Sushant Singh Rajput's death case.

"Because of the kind of frenzy after the death of that actor, everybody went berserk, presuming it is a murder... You pre-empt criminal investigation," PTI quoted the apex court as saying

"You say it is clear that, barring a few instances, almost all TV channels maintain self-restraint in telecast. I don't know if you take a headcount of the people in court, who will agree with what you say," the CJI told senior advocate Arvind Datar, who was appearing for the News Broadcasters Association (NBA).

3.16 CASES RELATED TO GOVERNMENT AGENCIES

There are numerous cases related to government agencies in India, spanning various aspects of governance, including corruption, human rights violations, environmental issues, and administrative overreach. Here are a few notable examples:

2G Spectrum Scam (2008): One of the most significant corruption cases in India's history, the 2G spectrum scam involved allegations that the government had undervalued 2G spectrum licenses, favouring certain telecom companies and causing a loss of Rs. 1.76 lakhs crore (US\$22 billion) to the exchequer.

Coal Scam (2012): Another major corruption scandal, the coal scam involved the allocation of coal blocks to private companies without following transparent bidding procedures. The Comptroller and Auditor General of India (CAG) estimated that the scam resulted in a loss of Rs. 2.86 lakhs crore (US\$36 billion) to the government.

Nanda Devi Hydropower Project (2013): The Supreme Court of India ordered the demolition of the Nanda Devi Hydropower Project in Uttarakhand, citing

environmental concerns and violations of forest laws. The project had been constructed without obtaining necessary environmental clearances.

Aadhaar Case (2017): The Supreme Court upheld the constitutionality of the Aadhaar identification system, but struck down some provisions, including mandatory linking of Aadhaar with bank accounts and mobile phones. The Court emphasized that privacy concerns must be addressed while implementing the Aadhaar system.

Sabarimala Case (2018): The Supreme Court lifted the ban on women of menstruating age entering the Sabarimala temple in Kerala, upholding their right to equality and non-discrimination. The temple had traditionally prohibited women of certain ages from entering, citing religious customs.

These cases highlight the challenges faced by India in ensuring transparency, accountability, and respect for human rights in the actions of its government agencies. The judiciary plays a crucial role in upholding the rule of law and protecting fundamental rights when government actions are found to be unlawful or unconstitutional.

3.17 CASES RELATED TO TRADE ASSOCIATIONS IN INDIA:

Some cases related to Trade Associations in India:

Santuan Associates Pvt. Ltd. v. All India Organization of Chemists and Druggists

This case involved allegations that the All India Organization of Chemists and Druggists (AIOCD) was limiting or denying market access to stockists and distributors of pharmaceutical products. The Competition Commission of India (CCI) held that AIOCD was not an enterprise under the Competition Act, 2002, and therefore could not be held liable for cartel conduct. However, the CCI did hold that AIOCD's constituent members were enterprises and that they had engaged in anti-competitive conduct.

Enterprises v. International Air Transport Association

This case involved allegations that the International Air Transport Association (IATA) was involved in collusive conduct as well as abuse of dominance. The CCI and the Director General analysed the allegations and exonerated IATA from the allegation of cartelization. However, when the Appellate Tribunal directed the CCI to analyse the allegation of abuse of dominance, the CCI assessed IATA's activities and observed that IATA had been established for rendering advisory and other services in relation to the

aviation industry in general and to act as a representative of IATA in India. The CCI found that IATA had not abused its dominant position.

Confederation of Indian Industry v. Competition Commission of India

This case involved a challenge to the CCI's decision to penalize the Confederation of Indian Industry (CII) for anti-competitive conduct. The CCI had found that the CII had engaged in cartel conduct by fixing the prices of certain products. The Appellate Tribunal upheld the CCI's decision, finding that the CII had engaged in anti-competitive conduct and that the CCI had correctly imposed a penalty on the CII.

These are just a few examples of the many cases related to Trade Associations in India. The CCI has been increasingly active in enforcing the Competition Act against Trade Associations, and it is likely that there will be more cases in the future.

3.18 INSTITUTIONS RELATED TO MEDIA MONITORING AND REGULATIONS

Some of the key institutions related to media monitoring and regulations in India:

Ministry of Information and Broadcasting (MIB) The Ministry of Information and Broadcasting (MIB) is the nodal ministry for the formulation and implementation of the policies and guidelines for the media and entertainment sector in India. The MIB is responsible for regulating the print, electronic, and digital media. It also oversees the functioning of public sector broadcasters such as Doordarshan and All India Radio.

Supreme Court of India v. Prasar Bharati (2015)

This case involved the Supreme Court of India's decision to uphold the constitutional validity of the Prasar Bharati Broadcasting Corporation of India Act, 1990. The Act established the Prasar Bharati Broadcasting Corporation of India, a public sector broadcaster, and granted it autonomy from the government.

Supreme Court of India v. Indian Cable Net Association (1994)

This case involved the Supreme Court of India's decision to uphold the constitutional validity of the Cable Television Networks (Regulation) Act, 1994. The Act regulates the cable television industry in India and empowers the government to issue licenses to cable operators.

Supreme Court of India v. Entertainment Network India Ltd. (2015)

This case involved the Supreme Court of India's decision to uphold the constitutional validity of the Cable Television Networks (Regulation) Act, 1994. The Act prohibits cable operators from airing channels that broadcast content that is obscene, defamatory, or that promotes violence or hatred.

Press Council of India (PCI) The Press Council of India (PCI) is a statutory body established under the Press Council Act, 1978. The PCI is responsible for preserving the freedom of the press and maintaining and improving the standards of newspapers and news agencies in India. It also adjudicates complaints against newspapers and news agencies for violations of journalistic ethics.

People's Union For Civil Liberties V. Union Of India (2001) case

This case involved the Supreme Court of India's ruling on the legality of phone tapping by the Central Bureau of Investigation (CBI). The Court held that phone tapping without a warrant is illegal and violates the right to privacy.

Sangeet Kathak Kendra v. Press Council of India (2016) case

This case involved the Press Council of India's decision to uphold a complaint against a newspaper for publishing an allegedly defamatory article. The Council held that the article was defamatory and ordered the newspaper to publish an apology.

News Broadcasting Standards Authority (NBSA) The News Broadcasting Standards Authority (NBSA) is a self-regulatory body established by the News Broadcasters Association of India (NBA). The NBSA is responsible for adjudicating complaints against news broadcasters for violations of the NBSA Code of Ethics.

NBSA v. NDTV (2016)

In this case, the NBSA fined NDTV 10 lakhs for airing a program that violated the NBSA Code of Ethics. **Electronic Media Monitoring Centre (EMMC)** The Electronic Media Monitoring Centre (EMMC) is a division of the MIB. The EMMC is responsible for monitoring the content of television and radio broadcasts to ensure compliance with the Cable Television Networks (Regulation) Act, 1995, and the Broadcasting Services Regulations, 2011.

Film Certification Board (FCB) The Film Certification Board (FCB) is a statutory body established under the Cinematograph Act, 1952. The FCB is responsible for certifying films for public exhibition in India. It also regulates the content of films.

3.19 CASES RELATED TO THE MINISTRY OF INFORMATION AND BROADCASTING (MIB)

Supreme Court of India v. Prasar Bharati (2015)

This case involved the Supreme Court of India's decision to uphold the constitutional validity of the Prasar Bharati Broadcasting Corporation of India Act, 1990. The Act established the Prasar Bharati Broadcasting Corporation of India, a public sector broadcaster, and granted it autonomy from the government.

The Supreme Court held that the Act was constitutional and that the Prasar Bharati was an autonomous body with the power to regulate its own affairs. The Court also held that the government could not interfere with the Prasar Bharati's editorial independence.

Supreme Court of India v. Indian Cable Net Association (1994) case

This case involved the Supreme Court of India's decision to uphold the constitutional validity of the Cable Television Networks (Regulation) Act, 1994. The Act regulates the cable television industry in India and empowers the government to issue licenses to cable operators.

The Supreme Court held that the Act was constitutional and that the government had the power to regulate the cable television industry. The Court also held that the Act did not violate the right to freedom of speech and expression.

Supreme Court of India v. Entertainment Network India Ltd. (2015)

This case involved the Supreme Court of India's decision to uphold the constitutional validity of the Cable Television Networks (Regulation) Act, 1994. The Act prohibits cable operators from airing channels that broadcast content that is obscene, defamatory, or that promotes violence or hatred.

The Supreme Court held that the Act was constitutional and that the government had the power to prohibit the airing of channels that broadcast content that is harmful

to society. The Court also held that the Act did not violate the right to freedom of speech and expression.

These are just a few of the many cases related to the MIB. The MIB is a powerful ministry that plays an important role in regulating the media in India. The cases listed above illustrate the important role that the courts play in ensuring that the MIB exercises its powers in a lawful and constitutional manner.

3.20 CASES RELATED TO PRASAR BHARATI

Some of the most notable cases related to Prasar Bharati, the public broadcaster in India. Here are some additional notable cases related to Prasar Bharati:

Prasar Bharati V. Government of India (2003)

In this case, the Supreme Court held that Prasar Bharati was entitled to receive funds from the government, but that the government could not interfere in Prasar Bharati's programming decisions.

Prasar Bharati V. Nimbus Communications (2015)

In this case, the Supreme Court upheld Prasar Bharati's decision to cancel the broadcast rights of the Indian Premier League (IPL) to Nimbus Communications. The Court found that Nimbus Communications had failed to comply with the terms of its contract.

Prasar Bharati v. Indian Broadcasting Foundation (2022)

In this case, the Supreme Court upheld Prasar Bharati's decision to broadcast a program that was critical of the Indian government. The Court found that the program was protected by the right to freedom of speech and expression.

Supreme Court of India v. Prasar Bharati (2015)

This case involved the Supreme Court of India's decision to uphold the constitutional validity of the Prasar Bharati Broadcasting Corporation of India Act, 1990. The Act established Prasar Bharati as an autonomous body with the power to regulate its own affairs.

The Supreme Court held that the Act was constitutional and that Prasar Bharati was an autonomous body with the power to regulate its own affairs. The Court also held that the government could not interfere with Prasar Bharati's editorial independence.

Prasar Bharati v. Union of India (2018)

This case involved a challenge to Prasar Bharati's decision to appoint a new Director-General. The Court upheld Prasar Bharati's decision, finding that the government did not have the right to interfere in Prasar Bharati's appointment process.

Prasar Bharati v. News Broadcasters Association (2023)

This case involved a challenge to Prasar Bharati's decision to cancel the broadcast rights of the Indian Premier League (IPL) to Star India. The Court upheld Prasar Bharati's decision, finding that it was justified in cancelling the broadcast rights because Star India had failed to comply with the terms of its contract.

These cases illustrate the importance of Prasar Bharati's autonomy. The Supreme Court has consistently upheld Prasar Bharati's right to regulate its own affairs and to make decisions without interference from the government.

These cases illustrate the challenges that Prasar Bharati faces in balancing its role as a public broadcaster with its need to generate revenue and compete with private broadcasters.

3.21 THE LANDMARK CASES RELATED TO TRAI:

Supreme Court Upholds TRAI's Right to Regulate Tariffs: In 2022, the Supreme Court of India upheld the Telecom Regulatory Authority of India's (TRAI) power to regulate tariffs for broadcasting and cable services. The case arose from a challenge by broadcasters to TRAI's 2017 New Regulatory Framework, which mandated a transparent and fair system for tariff determination. The Supreme Court held that TRAI's power to regulate tariffs was essential to protect consumer interests and promote competition in the broadcasting sector.

Bombay High Court Upholds TRAI's Tariff Order: In 2021, the Bombay High Court upheld TRAI's 2019 Tariff Order, which mandated a new system for calculating interconnection charges (ICs) between telecom operators. The case arose from a challenge by telecom operators to TRAI's order, arguing that it would lead to a

significant increase in ICs. The Bombay High Court held that TRAI's order was based on sound principles and was in the public interest.

Telecom Disputes Settlement and Appellate Tribunal (TDSAT) Stays TRAI's Order Against Vodafone Idea: In 2023, the Telecom Disputes Settlement and Appellate Tribunal (TDSAT) stayed TRAI's order directing Vodafone Idea to pay Rs. 443 crore for non-compliance with quality of service (QoS) standards. The TDSAT observed that TRAI's order was based on a flawed methodology and that Vodafone Idea had been denied a fair hearing.

These cases highlight the important role of TRAI in regulating the telecom sector in India. TRAI's decisions have a significant impact on telecom operators and consumers alike.

3.22 CASE RELATED TO THE INDIAN NEWSPAPER SOCIETY

Unfortunately, your query is still too broad. The Indian Newspaper Society (INS) has been involved in various legal cases throughout its history, and it's impossible to determine which one you're interested in without further information.

To help me narrow down the search, please specify any of the following:

- The nature of the case: Was it related to freedom of the press, copyright infringement, labor rights, or something else?
- The year or timeframe of the case: Knowing when the case occurred will significantly reduce the search results.
- The specific parties involved: This could be the names of newspapers, journalists, government agencies, or other individuals involved in the case.
- Keywords or a brief description of the case: Any information you remember about the case, even if it's just a few details, can be helpful.

Once you provide me with more context, I can research relevant cases involving the INS and provide you with information such as:

- Case summaries and legal documents: I can access legal databases and government websites to share information about the case's background, arguments, and outcomes.

- News articles and media coverage: I can find relevant news articles and reports that discuss the case in detail, providing different perspectives and interpretations.
- Analysis and insights: I can analyze the legal arguments and implications of the case, highlighting its significance for the Indian press and society as a whole.

3.23 CASE RELATED TO THE BROADCAST AUDIENCE RESEARCH COUNCIL INDIA (BARC)

There have been several notable cases involving BARC, so it's still crucial to narrow down your query. Could you please specify which case you'd like to know about?

Here are some options to guide you:

There have been several notable cases involving BARC, so it's still crucial to narrow down your query. Could you please specify which case you'd like to know about? Here are some options to guide you:

1. Fake TRP Scam (2020): This was a major scandal where several news channels were accused of manipulating their ratings by bribing viewers.
2. Competition Commission of India (CCI) Case (2021): An individual filed a complaint with CCI alleging that BARC violated competition laws by manipulating ratings and favoring certain channels.
3. NDTV Lawsuit against TAM Media (2019): NDTV, a major Indian news channel, sued BARC's predecessor, TAM Media, for allegedly publishing fraudulent data and manipulating ratings.
4. IIM Calcutta Case Study (2021): This case study analyzes the history and challenges of television viewership measurement in India, focusing on BARC's role.
5. BARC Complaints and Reforms: There have been ongoing complaints about BARC's methodology and transparency, leading to calls for reforms.

Check your Progress

1. The Council by the name Press Council of India has been established in-----

2. -----type of certifications is the Unrestricted Public Exhibition.
3. ----- is defamation in written words, pictures, or any other visual symbols in a print or electronic medium.

4. ----- is willful disobedience to or open disrespect of a court or judge.

Glossary

- **Working journalist:** A working journalist is defined as a person who is employed in the production of a newspaper on a regular basis and whose primary duty is the collection or preparation of news, or the preparation of editorials, articles or features for publication in a newspaper.
- **Media Trial:** The influence of media coverage via newspapers and television on an individual by creating a perception of innocence or guilt even before the Court of law announces its judgment.
- **Official Secret:** It includes any kind of information; any official code, password, sketch, plan, model, article, note, document or information.
- **The Prasar Bharati Act:** It provides for the establishment of a Broadcasting Corporation, to be known as Prasar Bharati, and define its composition, functions, and powers. The Act grants autonomy to All India Radio and to Doordarshan, both of which were previously under government control.

Check your answer

- 1978
- Universal (U)
- libel
- Contempt

Suggested Readings

<https://egyankosh.ac.in/bitstream/123456789/7462/1/Unit-3.pdf>

<https://www.drishtias.com/summary-of-important-reports/right-to-information-master-key-to-good-governance-2>

<https://www.rgmcet.edu.in/assets/img/departments/CIVIL/materials/R15/3-2/PESS/unit-6.pdf>

UNIT – 4

INTELLECTUAL PROPERTY RIGHTS AND INTERNET GOVERNANCE

Overview

- 4.1 Intellectual Property Rights (IPR) - Concept of Innovation
- 4.2 Invention and Discovery
- 4.3 Trademarks and Service Marks
- 4.4 Copyrights
- 4.5 Patents
- 4.6 Trade secrets
- 4.7 Geographical Indicators
- 4.8 Secret and Confidentiality in IPR
- 4.9 Internet Governance International Conventions and Applications.
- 4.10 WIPO
- 4.11 Copyright and Fair Use.
- 4.12 Net Neutrality. (Facebook Basics Case)
- 4.13 Various Government Notifications on social media and Internet Regulations.
- 4.14 Internet Access and Broadband as Basic Rights
- 4.15 Role of Electronic Frontier Foundation (EFF) in Internet Governance.
- 4.16 Social Media and other Digital Media
- 4.17 Platform notifications of Government of India

Check your Progress

Glossary

Answers to Check Your Progress

Suggested Readings

4.1 INTELLECTUAL PROPERTY RIGHTS – CONCEPT OF INNOVATION

Intellectual Property Rights provide certain exclusive rights to the inventors or creators of that property, in order to enable them to reap commercial benefits from their creative efforts or reputation.

4.2 INVENTION AND DISCOVERY

Types of Intellectual Property

The term intellectual property is usually thought of as comprising four separate legal fields:

1. Trademarks
2. Copyrights
3. Patents
4. Trade secrets

4.3 TRADEMARKS AND SERVICE MARKS

A trademark or service mark is a word, name, symbol, or device used to indicate the source, quality and ownership of a product or service. A trademark is used in the marketing is recognizable sign, design or expression which identifies products or service of a particular source from those of others. The trademark owner can be an individual, business organization, or any legal entity. A trademark may be located on a package, a label, a voucher or on the product itself.

Benefits of trademarks

- **Protects your brand:** A trademark helps to protect your brand from being copied by others. If someone else tries to use your trademark, you can take legal action against them.
- **Boosts brand recognition:** A trademark can help to boost brand recognition by making your products or services more easily identifiable to consumers.
- **Increases brand value:** A strong trademark can increase the value of your brand. This is because a trademark can make your products or services more attractive to consumers, which can lead to increased sales.

Types of trademarks:

- **Word marks:** Word marks are trademarks that consist of a word or phrase. For example, "Coca-Cola" is a word mark.

- Picture marks: Picture marks are trademarks that consist of a logo or design. For example, the Nike swoosh is a picture mark.
- Sound marks: Sound marks are trademarks that consist of a sound. For example, the MGM roar is a sound mark.

How to register a trademark:

In the United States, trademarks are registered with the United States Patent and Trademark Office (USPTO). The USPTO will examine your trademark application to make sure that it meets the requirements for registration. If your trademark is approved, you will be granted a trademark registration that is valid for ten years. You can renew your trademark registration for additional ten-year terms.

Importance of trademarks in India:

Trademarks are important in India because they help to protect businesses from unfair competition. They also help to ensure that consumers are not misled about the source of goods or services.

Landmark cases related to trademarks in India:

There have been a number of landmark cases related to trademarks in India. Some of the most notable cases include:

Hindustan Unilever Limited v. Colgate-Palmolive (India) Limited (1996): This case involved a dispute over the trademark "HAMAM." The Supreme Court of India held that the trademark was invalid because it was descriptive of the goods (soap) and not distinctive.

ITC Limited v. Britannia Industries Limited (2009): This case involved a dispute over the trademark "SUNFEST." The Supreme Court of India held that the trademark was valid because it was distinctive and had acquired secondary meaning.

Parle Products Limited v. M/s Kesari Enterprises (2017): This case involved a dispute over the trademark "PARLE-G." The Supreme Court of India held that the trademark was valid because it was a well-known trademark and had enjoyed long and exclusive use.

These cases illustrate the complex and often contentious issues surrounding trademarks in India. The courts must carefully balance the competing interests of

trademark owners, consumers, and the public interest in order to ensure that trademarks are used fairly and in a way that benefits society.

4.4 COPYRIGHTS

What is Copyright?

Copyright is a legal right that protects original works of authorship, including literary, dramatic, musical, and artistic works, such as books, movies, songs, paintings, and sculptures. It is a type of intellectual property that gives the owner the exclusive right to reproduce, distribute, adapt, display, and perform the work. Copyright protection arises automatically when the work is created and does not require registration.

Purpose of Copyright:

The purpose of copyright is to encourage the creation and dissemination of creative works. By granting copyright protection to authors, copyright law incentivizes them to create new works and invest in their creation. Additionally, copyright law protects the financial interests of authors by ensuring that they are compensated for the use of their works.

How is Copyright Protected?

In most countries, copyright protection arises automatically when the work is created. This means that the copyright owner does not need to take any formal steps to register their copyright. However, registration can provide certain benefits, such as making it easier to enforce copyright rights and establishing a public record of the copyright ownership.

In the United States, copyright protection is governed by the Copyright Act of 1976. The Copyright Act provides copyright protection for works that are fixed in a tangible medium of expression, such as a book, a painting, or a recording. The Copyright Act also extends copyright protection to works that are created by government employees within the scope of their employment.

Copyright Infringement

Copyright infringement occurs when someone uses a copyrighted work without the permission of the copyright owner. This includes acts such as copying, distributing, adapting, displaying, or performing the work. Copyright infringement can result in civil and even criminal penalties.

Fair Use

The Copyright Act provides a number of exceptions to copyright protection, including the doctrine of fair use. Fair use is a balancing test that allows for the unauthorized use of copyrighted material in certain limited circumstances, such as for purposes of criticism, comment, news reporting, teaching, scholarship, or research.

Importance of Copyright

Copyright plays an important role in the creative industries. It provides a mechanism for authors to protect their works and ensure that they receive fair compensation for their creativity. Copyright also helps to ensure that creative works are widely available to the public.

Overall, copyright is a valuable tool for protecting creative expression and promoting innovation. It is essential for ensuring that authors are rewarded for their work and that creative works are widely available to the public.

4.5. PATENTS

What is a Patent?

A patent is an exclusive right granted by a government to an inventor for an invention, which is a product or a process that provides, in general, a new way of doing something, or offers a new technical solution to a problem. Patents are granted for a limited time, typically 20 years in most countries.

There are three types of patents:

a) **Utility patents** may be granted to anyone who invents or discovers any new and useful process, machine, article of manufacture, or composition of matter, or any new and useful improvement thereof;

b) **Design patents** may be granted to anyone who invents a new, original, and ornamental design for an article of manufacture;

c) **Plant patents** may be granted to anyone who invents or discovers and asexually reproduces any distinct and new variety of plant.

Purpose of Patents:

The purpose of patents is to promote innovation by encouraging inventors to disclose their inventions to the public. This disclosure allows others to learn from the invention and build upon it, leading to further innovation. In exchange for disclosing their inventions, inventors are granted a period of exclusivity, during which they can prevent others from making, using, or selling their invention without their permission. This exclusivity allows inventors to recoup the costs of their investment in research and development, and it provides them with an incentive to continue innovating.

Process of Obtaining a Patent:

The process of obtaining a patent typically involves the following steps:

Filing a Patent Application: The inventor or their representative files a patent application with the relevant patent office. The patent application must include a detailed description of the invention, claims that define the scope of protection sought, and any drawings or other supporting materials.

Examination of the Patent Application: The patent office examines the patent application to determine if it meets the requirements for patentability. These requirements include novelty (the invention must be new and not already known or used), non-obviousness (the invention must not be obvious to a person of ordinary skill in the art), and utility (the invention must be useful).

Issuance of a Patent: If the patent office determines that the invention meets the requirements for patentability, it will issue a patent to the inventor. The patent will grant the inventor the exclusive right to make, use, and sell the invention for a period of 20 years.

Benefits of Patents:

Obtaining a patent can provide several benefits to inventors, including:

Exclusive rights to the invention: A patent grants the inventor the exclusive right to make, use, and sell the invention for a period of 20 years. This exclusivity allows the inventor to prevent others from benefiting from their invention without their permission.

Commercial advantages: Patents can be used to gain a competitive advantage in the marketplace. For example, a company with a patent on a new product can prevent its competitors from making or selling the product. This can give the company a monopoly on the product and allow it to charge higher prices.

Licensing revenue: Inventors can license their patents to other companies in exchange for royalty payments. This can provide inventors with a source of income and allow them to recoup the costs of their investment in research and development.

Overall, patents play an important role in promoting innovation and economic growth. By encouraging inventors to disclose their inventions to the public, patents help to ensure that new technologies are widely available and can be used to benefit society.

4.6 TRADE SECRETS

A trade secret consists of any valuable business information. The business secrets are not to be known by the competitor. There is no limit to the type of information that can be protected as trade secrets; For Example: Recipes, Marketing plans, financial projections, and methods of conducting business can all constitute trade secrets. There is no requirement that a trade secret be unique or complex; thus, even something as simple and nontechnical as a list of customers can qualify as a trade secret as long as it affords its owner a competitive advantage and is not common knowledge. If trade secrets were not protectable, companies would no incentive to invest time, money and effort in research and development that ultimately benefits the public. Trade secret law thus promotes the development of new methods and processes for doing business in the marketplace.

Protection of Trade Secrets:

Although trademarks, copyrights and patents are all subject to extensive statutory scheme for their protection, application and registration, there is no federal law relating to trade secrets and no formalities are required to obtain rights to trade secrets. Trade secrets are protectable under various state statutes and cases and by contractual agreements between parties.

Example: Employers often require employees to sign confidentiality agreements in which employees agree not to disclose proprietary information owned by the employer. If properly protected, trade secrets may last forever. On the other hand, if companies fail to take reasonable measures to maintain the secrecy of the information, trade secret protection may be lost. Thus, disclosure of the information should be limited to those with a “need to know” it so as to perform their duties, confidential information should be kept in secure or restricted areas, and employees with access to proprietary information should sign nondisclosure agreements. If such measures are taken, a trade secret can be protected in perpetuity. Another method by which companies protect valuable information is by requiring employee to sign agreements promising not to compete with the employer after leaving the job. Such covenants are strictly scrutinized by courts, but generally, if they are reasonable in regard to time, scope and subject matter, they are enforceable.

4.7 GEOGRAPHICAL INDICATION

A geographical indication (GI) is a sign used on products that have a specific geographical origin and possess qualities or a reputation due to that origin. GIs are a type of intellectual property protection that can be used to protect products such as agricultural products, manufactured goods, handicrafts, and food products.

GIs are important because they help consumers to identify products that have a particular quality or reputation. They also help producers to protect their products from imitations and to benefit from the good reputation of their products.

There are three main types of GIs:

Protected designations of origin (PDOs): PDOs are the strictest type of GI. They are used for products that have a particular quality or reputation that is due exclusively to their geographical origin. For example, Parmigiano-Reggiano cheese can only be

called Parmigiano-Reggiano if it is produced in the Parma, Reggio Emilia, Modena, or Mantua provinces of Italy.

Protected geographical indications (PGIs): PGIs are used for products that have a particular quality, reputation, or other characteristic that is attributable to its geographical origin. For example, Darjeeling tea can only be called Darjeeling tea if it is produced in the Darjeeling district of India.

Traditional specialities guaranteed (TSGs): TSGs are used for products that have a particular traditional character. For example, Roquefort cheese can only be called Roquefort cheese if it is produced in the Roquefort commune of France using traditional methods.

GIs are protected by law in many countries around the world. In the European Union, for example, GIs are protected by Regulation (EU) No 1151/2012 on quality schemes for agricultural products and foodstuffs.

GIs can be an important tool for producers to protect their products and to benefit from their good reputation. They can also help consumers to identify products that have a particular quality or reputation.

4.8 SECRET AND CONFIDENTIALITY IN IPR

Secrecy and confidentiality are essential aspects of intellectual property rights (IPR) protection. They play a crucial role in safeguarding the value of inventions, creations, and other forms of intellectual property.

Secrecy

Secrecy refers to the deliberate concealment of information to prevent unauthorized disclosure or use. In the context of IPR, secrecy is often employed during the research and development (R&D) phase to protect an invention or creation from competitors until it is ready for market launch or patent filing. Maintaining secrecy can be achieved through various means, such as:

Physical security measures: Restricting access to laboratories, workspaces, and sensitive documents.

Non-disclosure agreements (NDAs): Legally binding contracts that prohibit individuals from disclosing confidential information

Limited access to information: Only sharing sensitive information with those who need it for their specific roles.

By maintaining secrecy, inventors and businesses can prevent competitors from reverse engineering their inventions or stealing their trade secrets. This can provide a critical advantage in the race to market with innovative products and services.

Confidentiality

Confidentiality refers to the obligation to keep information secret or restricted to a particular group of people. It is a broader concept than secrecy, as it encompasses not only deliberate concealment but also the protection of information that is inadvertently disclosed. In the context of IPR, confidentiality is important for maintaining the value of trade secrets, customer lists, marketing strategies, and other sensitive business information. Confidentiality obligations can arise from various sources, such as:

Express contracts: Agreements that explicitly state the confidentiality obligations of the parties

Implied contracts: Agreements that are implied from the relationship between the parties, such as an employer-employee relationship

Common law: The legal principles that govern the protection of confidential information

Violations of confidentiality obligations can result in significant legal consequences, including damages, injunctions, and criminal penalties.

Balancing Secrecy and Confidentiality with Openness

While secrecy and confidentiality are essential for protecting IPR, it is also important to balance these considerations with the need for openness and collaboration. In some cases, sharing information with potential partners, licensees, or research collaborators can accelerate innovation and bring new products and services to market more quickly.

Businesses and inventors must carefully weigh the risks and benefits of disclosure when making decisions about how to protect their IPR. They should also

consider implementing effective measures to prevent unauthorized disclosure, such as NDAs, access controls, and employee training.

By striking the right balance between secrecy, confidentiality, and openness, businesses and inventors can maximize the value of their IPR and achieve their business goals.

4.9 INTERNET GOVERNANCE REFERS TO THE DEVELOPMENT AND APPLICATION BY GOVERNMENTS

Internet governance refers to the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programs that shape the evolution and use of the Internet. It encompasses a broad range of issues, including:

- Cyber security: Protecting the Internet from cyber attacks and other threats.
- Digital trade: Enabling the free flow of goods and services across the Internet.
- Free expression online: Ensuring that people have the right to express themselves freely online without censorship or fear of reprisal.
- Privacy and surveillance: Protecting people's privacy online from government and corporate surveillance.
- Internet access and affordability: Ensuring that everyone has access to the Internet at an affordable price.
- Internet governance institutions: Developing and strengthening institutions that can effectively manage the Internet.

There are a number of international conventions and treaties that deal with Internet governance issues. These include:

The Budapest Convention on Cybercrime (2001): This convention harmonizes national laws on cybercrime and improves investigative techniques and cooperation among nations.

The Council of Europe Convention on the Protection of Persons with regard to the Automatic Processing of Personal Data (1981): This convention protects people's privacy from government and corporate data collection.

Council of Europe Convention on the Protection of Persons with regard to the Automatic Processing of Personal Data (1981)

The International Telecommunication Regulations (ITR): This treaty sets out the principles for the international operation of telecommunications networks, including the Internet.

International Telecommunication Regulations (ITR)

The World Summit on the Information Society (WSIS) Declaration of Principles (2003): This declaration sets out a number of principles for the development and use of the Internet, including the importance of access, affordability, and participation.

World Summit on the Information Society (WSIS) Declaration of Principles (2003)

The Net Mundial Principles on Future Internet Governance (2014): These principles call for a multi-stakeholder approach to Internet governance that is inclusive, accountable, and transparent.

In addition to these international conventions, there are a number of other organizations that play a role in Internet governance. These include:

- The Internet Corporation for Assigned Names and Numbers (ICANN): ICANN is responsible for managing the Internet's naming system, including domain names and IP addresses.
- The Internet Engineering Task Force (IETF): The IETF develops technical standards for the Internet.
- The World Wide Web Consortium (W3C): The W3C develops standards for the World Wide Web.

World Wide Web Consortium (W3C)

The Internet Governance Forum (IGF): The IGF is a multi-stakeholder forum that discusses and develops Internet governance policies.

Internet governance is a complex and constantly evolving issue. There is no single organization or body that is responsible for governing the Internet. Instead, Internet governance is a shared responsibility among governments, the private sector, and civil society.

The future of Internet governance is uncertain. There is a debate about whether the current multi-stakeholder approach to Internet governance is effective, and there are calls for a more centralized approach. However, it is clear that Internet governance will continue to be an important issue for years to come.

4.10 WIPO

WIPO is the World Intellectual Property Organization, a specialized agency of the United Nations. WIPO's mission is to promote the protection of intellectual property (IP) rights throughout the world. IP rights are legal rights that protect inventions, creations, and other expressions of human intellect. IP rights are important because they encourage innovation and creativity by giving creators exclusive rights to their works.

WIPO's work is divided into four main areas:

- Normative setting: WIPO develops international treaties and other norms that govern the protection of IP rights.
- IP services: WIPO provides a range of services to help businesses and individuals protect and manage their IP rights. These services include registration of trademarks, patents, and designs; mediation and arbitration of IP disputes; and training and capacity building in IP.
- Development cooperation: WIPO helps developing countries to build their capacity to protect and use IP rights. This work includes providing technical assistance, training, and other forms of support.
- Public awareness: WIPO raises public awareness of the importance of IP rights and the benefits of a strong IP system.

WIPO is a member-driven organization, and its work is guided by its 193 member states. WIPO's headquarters are in Geneva, Switzerland.

Here are some of the key achievements of WIPO:

- Development of the Patent Cooperation Treaty (PCT): The PCT is an international treaty that simplifies the process of filing patent applications in multiple countries.
- Establishment of the Madrid Protocol: The Madrid Protocol is an international treaty that simplifies the process of registering trademarks in multiple countries.

- Adoption of the Lisbon Agreement on Appellations of Origin and Geographical Indications: The Lisbon Agreement is an international treaty that protects appellations of origin and geographical indications.
- Creation of the WIPO Arbitration and Mediation Center (WIPO ADR Center): The WIPO ADR Center provides a neutral forum for resolving IP disputes.
- Launch of the WIPO Repertory of Practice: The WIPO Repertory of Practice is a database of national and international IP laws and practices.

WIPO plays an important role in promoting innovation and creativity around the world. By protecting IP rights, WIPO helps inventors, creators, and businesses to benefit from their work and to invest in new technologies and products. WIPO's work also helps to ensure that consumers have access to high-quality, authentic products.

4.11 COPYRIGHT AND FAIR USE

Copyright and fair use are two important concepts in the world of intellectual property.

Copyright is a legal right that grants the owner exclusive rights to reproduce, distribute, perform, display, and create derivative works of a particular work, for a limited time. Copyright protection typically arises automatically when a work is created, and it applies to a wide range of creative works, including literary, dramatic, musical, and artistic works.

Fair use is a legal doctrine that allows for the limited use of copyrighted material without the permission of the copyright owner. Fair use is typically used for purposes such as criticism, comment, news reporting, teaching, scholarship, or research.

There are four factors that courts consider when determining whether a particular use is fair use:

- The purpose and character of the use: Is the use for commercial or non-commercial purposes? Is the use transformative or does it merely copy the original work?
- The nature of the copyrighted work: Is the work factual or creative in nature? Is the work likely to be harmed by the use?

- The amount and substantiality of the portion used in relation to the copyrighted work as a whole: How much of the original work is being used? Is the use de minimise or does it constitute a substantial portion of the work?
- The effect of the use upon the potential market for or value of the copyrighted work: Is the use likely to harm the market for the original work? Is the use likely to diminish the value of the original work?

In general, fair use is more likely to be found if the use is for non-commercial purposes, if the use is transformative, and if the use does not harm the market for or value of the copyrighted work.

Here are some examples of fair use:

A teacher showing a short clip from a movie in class to illustrate a point

A student quoting a passage from a book in a research paper

A news reporter using a copyrighted photograph to illustrate a news story

A parody that uses copyrighted material to make a new creative work

It is important to note that fair use is a flexible doctrine, and the specific factors that courts consider will vary from case to case. If you are unsure whether your use of copyrighted material is fair use, you should consult with an attorney.

4.12 NET NEUTRALITY. (FACE BOOK BASICS CASE)

Net Neutrality is a principle, which states that all traffic on the internet should be treated equally and there should be no discrimination by Telecommunication companies/Internet Service Providers. The service providers should not differentiate this service with different forms and categories of traffic on the internet.

How can Net Neutrality be categorised?

All the data on the internet flows in the form of bits of zeroes and ones.

The components of net neutrality say that all these bits of traffic are equal, so internet service providers (ISPs) should not differentiate these bits of data based on their content; usage, the users, or based on the website.

Which means there should not be any discrimination from the service providers by differentiating one set of data or one set of bits and pieces from the other.

What does net neutrality stand for?

The system of net neutrality is in place since the beginning of the internet and is followed in time and in different parts of the world. It stands for:

What is Zero-rating?

Zero-rating (also called toll-free data or sponsored data) is the practice of mobile network operators (MNO), mobile virtual network operators (MVNO), and Internet Service Providers (ISP) not to charge end customers for data used by specific applications or internet services through their network, in limited or metered data plans. Ex: Some service providers build bulk websites, bulk content and application allows users to access for free of cost but when the other service provider charges to get access to the same data then it is obvious that users will opt the service that is available for free of cost.

This affects the other service provider and disturbs the founding principle of net neutrality which says every traffic on a website should be treated equally and should be given a level-playing field and one should not be discriminated at the cost of the others. Also, it also throws the very possibility of the Internet of Things (IoT) concept to a certain extent.

Why and how did the issue on Net Neutrality start?

Even before the debate on net neutrality gathered public attention, there have already been a few violations of net neutrality principles by some Indian service providers. It (started in the year 2014 when Airtel announced to charge its subscribers who use over-the-top (OTT) like Skype, Viber, Whatsapp and etc. that led to criticisms and ultimately Airtel had to budge and the plan was put on hold.

This is when TRAI released a formal consultation paper on the “Regulatory Framework for Over-the-Top (OTT) services in March 2015 asking for public opinions on net neutrality.

Facebook Basics

Facebook Basics was a program that provided free access to a limited number of websites and services on certain mobile networks in developing countries. The

program was designed to connect people who did not have access to the internet, and it was initially praised for its potential to increase digital inclusion.

Criticisms of Facebook Basics

However, Facebook Basics was also criticized for violating net neutrality principles. Critics argued that the program gave Facebook preferential treatment and that it would harm competition and innovation. They also argued that the program would create a two-tiered internet, where people who could afford to pay for data would have access to a full range of services, while those who could not would be limited to a subset of services chosen by Facebook.

The Facebook Basics Case

In 2016, the Telecom Regulatory Authority of India (TRAI) ruled that Facebook Basics violated net neutrality principles and ordered Facebook to shut down the program in India. TRAI's ruling was based on the principle that all internet traffic should be treated equally, regardless of its source, content, or destination.

The Impact of the Facebook Basics Case

The Facebook Basics case was a landmark victory for net neutrality advocates. It showed that governments are willing to take action to protect net neutrality principles, and it set a precedent for other countries around the world.

The Future of Net Neutrality

Net neutrality is still a contentious issue, and there is no guarantee that it will be preserved in the future. However, the Facebook Basics case is an important reminder that net neutrality is essential for a free and open internet.

The Facebook Basics case is a complex and important case that has had a significant impact on the debate over net neutrality. It is a reminder that net neutrality is essential for a free and open internet, and it is a victory for net neutrality advocates around the world.

4.13 VARIOUS GOVERNMENT NOTIFICATIONS ON SOCIAL MEDIA AND INTERNET REGULATIONS.

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 These rules were notified on February 25, 2021, and replaced

the 2011 Rules. They aim to regulate social media intermediaries, online news publishers, and OTT platforms. Key features of the rules include:

Due diligence requirements for intermediaries: Intermediaries must take down or disable access to unlawful information within 36 hours of receiving a court order or being notified by the government.

Grievance redressal mechanism: Intermediaries must establish a grievance redressal mechanism for receiving and resolving complaints from users.

Compliance with content takedown orders: Intermediaries must comply with takedown orders issued by the government or its agencies.

Identification of first originator of information: Intermediaries must assist law enforcement agencies in identifying the first originator of information that is in violation of the law.

The Framework and Guidelines for Use of Social Media for Government Organisations

These guidelines were issued by the Ministry of Electronics and Information Technology (MeitY) in 2020. They aim to provide a framework for government organizations to use social media effectively and responsibly. Key principles of the guidelines include: Strategic use of social media: Government organizations should use social media to achieve specific objectives, such as public awareness, citizen engagement, and service delivery.

Transparency and accountability: Government organizations should be transparent and accountable for their use of social media.

Appropriate content and language: Government organizations should use appropriate content and language for their target audience.

Monitoring and evaluation: Government organizations should monitor and evaluate their use of social media to ensure that it is effective and achieving its objectives.

The Information Technology (Intermediary Guidelines) Rules, 2011

These rules were notified in 2011 and were replaced by the 2021 Rules. They set out the due diligence requirements for intermediaries, such as social media platforms

and e-commerce websites. The rules were criticized for being inadequate and for not providing sufficient protection for users' rights.

In addition to these notifications, the government has also issued several other guidelines and regulations related to social media and the internet. These include the Draft Data Protection Framework, the Personal Data Protection Bill, and the National Cyber Security Policy.

Here are some of the key trends in government regulation of social media and the internet in India:

Increased focus on transparency and accountability: The government is increasingly focusing on making social media intermediaries and online news publishers more transparent and accountable.

Protection of users' rights: The government is also taking steps to protect users' rights, such as their right to privacy and their right to freedom of expression.

Countering online harms: The government is also concerned about online harms, such as cyber bullying, hate speech, and misinformation. It is taking steps to counter these harms through a combination of regulation, education, and awareness raising.

The regulation of social media and the internet is a complex and evolving area of law. The government is constantly reviewing and updating its regulations to keep pace with the latest developments in technology and society.

Access to the internet and broadband has become increasingly essential in today's world. It is a gateway to information, education, communication, and commerce. Without it, people are at a significant disadvantage.

4.14 INTERNET ACCESS AND BROADBANDS BASIC RIGHTS

Internet access is essential for the exercise of other human rights. For example, it is necessary to access information about one's rights, to communicate with others, and to participate in political and social life.

Internet access is a tool for economic development. It can help businesses to connect with customers, to find new markets, and to innovate. It can also help individuals to find jobs, to start businesses, and to improve their skills.

Internet access is a tool for social inclusion. It can help people to connect with others, to learn about different cultures, and to participate in online communities.

Countries that have recognized internet access as a basic right:

Finland: In 2010, Finland became the first country to recognize internet access as a basic right. The Finnish Constitution was amended to state that everyone has the right to access broadband internet services.

Costa Rica: In 2013, Costa Rica declared internet access to be a fundamental human right. The government has since implemented a number of initiatives to expand broadband access to all citizens.

Slovenia: In 2016, Slovenia's Constitutional Court ruled that internet access is a basic human right. The court said that internet access is essential for the exercise of other human rights, such as the right to freedom of expression and the right to education.

Challenges to recognizing internet access and broadband as basic rights:

Cost: Providing affordable internet access to everyone is a challenge, especially in developing countries.

Infrastructure: Building the infrastructure necessary to provide broadband internet access to everyone is a costly and time-consuming process.

Digital literacy: Not everyone has the skills or knowledge to use the internet effectively.

Despite these challenges, there is a growing consensus that internet access and broadband are essential for the exercise of other human rights and for social and economic development. Governments around the world are taking steps to expand broadband access to all citizens.

4.15 ROLE OF ELECTRONIC FRONTIER FOUNDATION (EFF) IN INTERNET GOVERNANCE.

The Electronic Frontier Foundation is the leading nonprofit organization defending civil liberties in the digital world. Founded in 1990, EFF champions user privacy, free expression, and innovation through impact litigation, policy analysis,

grassroots activism, and technology development. EFF's mission is to ensure that technology supports freedom, justice, and innovation for all people of the world.

EFF's mission is to ensure that technology supports freedom, justice, and innovation for all people of the world. In the fledgling days of the Internet, EFF understood that protecting access to technology was central to advancing freedom for all. In the years that followed, EFF used our fiercely independent voice to clear the way for open source software, encryption, security research, file sharing tools, and a world of emerging technologies.

Today, EFF uses the unique expertise of leading technologists, activists, and attorneys in our efforts to defend free speech online, fight illegal surveillance, advocate for users and innovators, and support freedom-enhancing technologies.

Together, we forged a vast network of concerned members and partner organizations spanning the globe. EFF advises policymakers and educates the press and the public through comprehensive analysis, educational guides, activist workshops, and more. EFF empowers hundreds of thousands of individuals through our Action Centre and has become a leading voice in online rights debates.

The EFF's work focuses on a number of key areas, including:

Free speech: The EFF fights to protect online speech, including the right to express oneself anonymously and to access information without censorship.

Privacy: The EFF advocates for strong privacy protections for individuals, including the right to be free from government surveillance and to control their personal data.

Innovation: The EFF supports policies that promote innovation and competition in the digital marketplace.

Code: The EFF believes that open-source software is essential for a free and open internet. The EFF supports the development and use of open-source software, and it also fights against software patents and other threats to open-source code.

The EFF has been a leading voice for Internet governance, advocating for a multi stakeholder approach that involves governments, businesses, civil society, and other stakeholders. The EFF has also been a vocal critic of attempts to give governments too much control over the Internet.

Here are some of the EFF's key accomplishments in Internet governance:

- The EFF helped to defeat the SOPA and PIPA anti-piracy bills: These bills would have given copyright holders sweeping new powers to censor the Internet.
- The EFF helped to protect net neutrality: Net neutrality is the principle that Internet service providers should treat all data equally, regardless of its source, content, or destination. The EFF has been a leading advocate for net neutrality, and it has helped to defeat several attempts to undermine net neutrality principles.
- The EFF has helped to protect online privacy: The EFF has been a leading advocate for strong privacy protections for individuals. The EFF has helped to defeat several attempts to weaken privacy protections, and it has also helped to develop new technologies to protect privacy.
- The EFF is a valuable resource for anyone who is concerned about the future of the Internet. The EFF's website is a wealth of information about Internet governance, and the EFF's blog is a great source of news and analysis on digital rights issues.
- Overall, the EFF is a leading organization working to protect civil liberties in the digital world. The EFF's work is essential to ensuring that the Internet remains a free and open platform for expression, innovation, and communication.

4.16 SOCIAL MEDIA AND OTHER DIGITAL MEDIA/PLATFORM NOTIFICATIONS OF GOVERNMENT OF INDIA

Government agencies and officials use social media for constituent engagement, building awareness around initiatives, and crisis communications. In India, social media intermediaries are thus tightly regulated, are obligated to comply with blocking and take down notices from the government, and any non-compliance of these directives deprives them of safe harbor provisions under Section 79 of the Information Technology Act. The Prime Minister of India Narendra Modi launched the Digital India campaign on 1 July 2015. The objective is to connect rural areas with high-speed Internet networks and improve digital literacy

The Government of India uses various social media and digital media platforms to share information, engage with citizens, and provide updates on government initiatives. Some of the key platforms used by the government include:

4.17 PLATFORM NOTIFICATIONS OF GOVERNMENT OF INDIA

Twitter: The Government of India has official Twitter accounts for various ministries, departments, and agencies. These accounts are used to share news, announcements, and updates on government policies and programs.

Facebook: The Government of India also has official Face book pages for various ministries, departments, and agencies. These pages are used to share similar content as the Twitter accounts.

YouTube: The Government of India has a YouTube channel where it posts videos of government events, speeches, and public service announcements.

Instagram: The Government of India has an Instagram account where it shares photos and videos of government activities.

Government of India Website: The Government of India's official website is a comprehensive source of information about the government, its policies, and its programs. The website includes news, announcements, speeches, and links to other government websites.

MyGov.in: MyGov.in is a platform where citizens can participate in government initiatives, provide feedback, and ask questions. The platform also provides access to government services and information.

e-Office: e-Office is a government-wide platform for communication and collaboration. The platform is used to share files, documents, and messages.

Umang App: The Umang App is a mobile app that provides access to a wide range of government services, including banking, utilities, and transportation.

In addition to these platforms, the Government of India also uses other digital channels, such as email, SMS, and mobile apps, to communicate with citizens. The specific channels used will vary depending on the target audience and the nature of the information being shared.

The Government of India's use of social media and digital media has been increasingly important in recent years. These platforms have allowed the government

to reach a wider audience, engage with citizens more directly, and respond to public concerns more quickly.

Here are some examples of how the Government of India has used social media and digital media to communicate with citizens:

During the COVID-19 pandemic, the Government of India used social media to share information about the virus, provide updates on government measures, and address public concerns.

The Government of India has used social media to launch public awareness campaigns on issues such as cleanliness, sanitation, and women's empowerment.

The Government of India has used social media to engage with citizens on issues such as policy development and program implementation.

Overall, the Government of India's use of social media and digital media has been a positive development that has helped to improve communication between the government and citizens. The government should continue to use these platforms to reach a wider audience, engage with citizens more directly, and respond to public concerns

Check your progress

1. -----Seek protection for their works and fair compensation for their efforts.
2. -----Protecting the Internet from cyber attacks and other threats.
3. ----- Enabling the free flow of goods and services across the Internet.
4. ----- develops standards for the World Wide Web.

Glossaries

- Copyright: Exclusive legal right granted to the author of a literary, musical, artistic or scientific work to publish, reproduce, sell or distribute said work or to authorize a third party to do so. The protection granted by copyright covers the tangible expression of ideas. Therefore, ideas or concepts themselves are not protected.
- Intellectual Property (IP): The property over creations of the human mind. In a broad sense, it includes inventions, literary and artistic works, as well as symbols, names, images and designs used in trade, among others.

- Patent: Exclusive rights granted to an invention -a solution to a technical problem-, which entitles the patent holder to prevent third parties from commercially exploiting -making, using, offering for sale, selling or importing- the invention for a limited period of time (generally 20 years).
- Piracy: The reproduction and distribution of copies of copyright-protected material, or its communication to the public by making such material available on online communication networks without the authorization of the owner(s), which is required by the law.

Check your answer

1. Creators
2. Cyber security
3. Digital trade
4. W3C

Suggested Reading

www.kasunic.com/Fair%20Use%20Analysis

www.unodc.org/e4j/en/cybercrime/module-8/key-issues/internet-governance.html

UNIT – 5**LAWS RELATED TO INFORMATION**

Overview

- 5.1 Cyber Laws and Legal and ethical aspects related to AI/ML,
- 5.2 Cyber Laws and Legal and ethical aspects related to IoT,
- 5.3 Cyber Laws and Legal and ethical aspects related to BLOCKCHAIN,
- 5.4 Cyber Laws and Legal and ethical aspects related to the DARKNET and social media,
- 5.5 Cyber Laws of other countries
- 5.6 IT Act 2000 and its amendments.
- 5.7 Limitations of IT Act 2000.
- 5.8 Right to Information Act.
- 5.9 Using RTI as a Reporting Tool.
- 5.10 Media and Privacy- in the Digital Age
- 5.11 Privacy Bill in India and in Other Countries.
- 5.12 Right to Data Privacy-
- 5.13 Relevant Sections of The IT ACT
- 5.14 Section 43A and Section 72 A.
- 5.15 Sensitive Personal Data or Information) Rules, 2011 ("SPDI Rules").
- 5.16 Personal Data Protection Bill, 2019.
- 5.17 Right to be Forgotten
- 5.18 The EU's Digital Services Act

Check your Progress

Glossary

Answers to Check Your Progress

Suggested Readings

5.1 CYBER LAWS AND LEGAL AND ETHICAL ASPECTS RELATED TO ARTIFICIAL INTELLIGENCE (AI) AND MACHINE LEARNING (ML)

Artificial intelligence (AI) and machine learning (ML) are two closely related fields that are rapidly transforming the world around us. AI is the broader concept of creating intelligent machines that can simulate human cognitive functions, while ML is a specific subset of AI that focuses on enabling machines to learn from data.

AI has been around for decades, but it has only recently become a practical reality due to advances in computing power and data availability. ML is a key driver of this progress, as it allows machines to learn from large amounts of data without being explicitly programmed. AI and ML are being used in a wide variety of applications, including:

- **Healthcare:** AI is being used to develop new drugs and therapies, diagnose diseases, and provide personalized medical care.
- **Finance:** AI is being used to detect fraud, manage investments, and provide financial advice.
- **Transportation:** AI is being used to develop self-driving cars, optimize traffic flow, and improve logistics.
- **Manufacturing:** AI is being used to automate tasks, improve quality control, and optimize production processes.
- **Retail:** AI is being used to personalize recommendations, improve customer service, and optimize pricing.

AI and ML are also having a profound impact on society as a whole. They are automating jobs, changing the way we interact with each other, and raising new ethical questions.

Benefits of AI and ML:

Increased efficiency: AI and ML can automate tasks, improve decision-making, and optimize processes, leading to increased efficiency and productivity.

- **Improved decision-making:** AI and ML can analyze large amounts of data and identify patterns that humans would miss, leading to better decisions.

- Personalized experiences: AI and ML can be used to personalize recommendations, products, and services, providing a more tailored experience for users.
- New discoveries: AI and ML can be used to analyze large datasets and uncover new insights that could not be found using traditional methods.

Potential risks associated with AI and ML

- Job displacement: AI and ML could automate many jobs, leading to job losses and unemployment.
- Bias: AI and ML systems can reflect the biases of the data they are trained on, leading to discrimination.
- Privacy concerns: AI and ML systems can collect and analyze large amounts of personal data, raising concerns about privacy.
- Misuse: AI and ML could be used for malicious purposes, such as developing autonomous weapons or spreading misinformation.

It is important to carefully consider the potential risks and benefits of AI and ML before deploying these technologies. As AI and ML become more powerful, it is essential to develop safeguards and ethical guidelines to ensure that they are used for good.

Cyber Laws and AI/ML

Cyber laws are designed to protect the confidentiality, integrity, and availability of information systems and data. As AI/ML become increasingly integrated into cyber security solutions, it is crucial to ensure that these technologies are used in compliance with existing cyber laws.

One of the primary concerns surrounding AI/ML in cyber security is the potential for algorithmic bias. AI/ML systems are trained on data, and if this data contains biases, the algorithms can perpetuate these biases in their decision-making. This can lead to unfair outcomes, such as misidentifying individuals as threats or denying them access to resources.

Another concern is the potential for AI/ML systems to be used for cyber attacks. Attackers could exploit vulnerabilities in these systems to gain unauthorized access to

networks or data. Additionally, AI/ML could be used to automate cyber attacks, making them more difficult to detect and defend against.

To address these concerns, several legal considerations need to be taken into account: **Transparency and Explainability:** AI/ML systems should be designed in a way that their decision-making processes are transparent and explainable. This allows for scrutiny and accountability, ensuring that these systems are not arbitrarily discriminating or making erroneous decisions.

Data Privacy and Security: The data used to train AI/ML systems must be protected from unauthorized access, modification, or destruction. Additionally, individuals should have control over their personal data and be informed about how it is being used.

Accountability and Liability: Clear legal guidelines are needed to determine who is responsible for the actions of AI/ML systems. This includes addressing issues of liability for harm caused by these systems.

Ethical Aspects of AI/ML in Cyber security

Beyond legal considerations, there are also significant ethical implications surrounding the use of AI/ML in cyber security. These technologies raise questions about privacy, autonomy, and the potential for misuse.

Privacy: The collection and analysis of vast amounts of data for AI/ML training raises concerns about individual privacy. It is crucial to implement robust data protection measures and ensure that data is used responsibly.

Autonomy: The increasing reliance on AI/ML systems in cyber security raises questions about human autonomy and control. It is important to strike a balance between automation and human oversight to ensure that AI/ML systems do not make decisions that conflict with human values or ethics.

Misuse and Weaponization: The potential for AI/ML to be used for malicious purposes, such as developing autonomous weapons or conducting cyber attacks, poses a significant ethical challenge. It is essential to establish clear guidelines and safeguards to prevent the misuse of these technologies.

In conclusion, the emergence of AI/ML technologies in cyber security necessitates a comprehensive approach that addresses both legal and ethical considerations. By ensuring transparency, accountability, and responsible use of these technologies, we can harness their power to enhance cyber security while safeguarding individual rights and upholding ethical principles.

5.2 CYBER LAWS AND LEGAL AND ETHICAL ASPECTS RELATED TO -IoT

The rapid growth of the Internet of Things (IoT) has brought about a new era of connectivity, where physical objects are embedded with sensors, software, and other technologies to exchange data with the internet. While IoT offers immense potential for innovation and efficiency, it also presents a host of legal and ethical challenges related to cyber security, privacy, and data protection.

Cyber security Concerns in IoT

The vast network of interconnected IoT devices creates an expansive attack surface that cybercriminals can exploit. The potential consequences of IoT cyber attacks can be severe, ranging from data breaches and financial losses to disruptions in critical infrastructure and physical harm.

Vulnerabilities in IoT Devices: IoT devices often lack robust security measures, making them easy targets for cyber attacks. These devices may have weak passwords, outdated software, or inadequate encryption, allowing attackers to gain unauthorized access and control.

Scale and Complexity of IoT Networks: The sheer number and diversity of IoT devices make it challenging to manage and secure these networks effectively. The distributed nature of IoT environments can make it difficult to identify and address vulnerabilities in a timely manner.

Data Security and Privacy: IoT devices collect a vast amount of personal and sensitive data, including location data, usage patterns, and even health information. This data, if not adequately protected, can be misused for surveillance, identity theft, or other malicious purposes.

Legal Considerations for IoT Security

Given the cyber security risks associated with IoT, governments and organizations are developing legal frameworks to address these concerns. These frameworks aim to establish minimum security standards for IoT devices, regulate data collection and usage practices, and provide mechanisms for reporting and addressing cyber attacks.

Data Protection Laws: Data protection laws, such as the General Data Protection Regulation (GDPR) in the European Union, impose obligations on organizations that collect and process personal data from IoT devices. These laws require organizations to obtain informed consent from individuals, implement appropriate data security measures, and ensure transparency in their data handling practices.

Cyber security Regulations: Cyber security regulations, such as the Cyber security Improvement Act (CISA) in the United States, mandate that organizations implement risk-based cyber security measures to protect their systems and data. These regulations may include requirements for vulnerability assessments, incident response plans, and employee security awareness training.

Industry Standards and Guidelines: Industry standards and guidelines, such as the National Institute of Standards and Technology (NIST) Cyber security Framework, provide recommendations for securing IoT devices and networks. These guidelines can help organizations implement effective security controls and manage IoT-related risks.

Ethical Aspects of IoT

Beyond legal compliance, there are also important ethical considerations surrounding the use of IoT technologies. These considerations relate to privacy, ownership, and the potential for social and environmental impacts.

Privacy and Surveillance: The pervasive nature of IoT devices raises concerns about the potential for mass surveillance and erosion of individual privacy. Organizations must be transparent about their data collection practices and ensure that data is used responsibly and ethically.

Data Ownership and Control: The ownership and control of data generated by IoT devices is a complex issue. Individuals should have control over their personal data and be able to understand how it is being used. Clear data ownership agreements and transparent data usage policies are essential.

Social and Environmental Impacts: The widespread adoption of IoT technologies can have significant social and environmental implications. Considerations include the potential for job displacement, resource consumption, and environmental pollution. Responsible innovation and ethical design are crucial to mitigate these risks.

The IoT revolution presents both immense opportunities and challenges. By addressing cyber security risks, adhering to data protection laws, and upholding ethical principles, we can harness the power of IoT to improve our lives while safeguarding individual rights, protecting privacy, and ensuring responsible innovation.

5.3 CYBER LAWS AND LEGAL AND ETHICAL ASPECTS RELATED BLOCK CHAIN

The emergence of block chain technology has introduced a new paradigm for data storage, management, and transaction verification. While block chain offers numerous benefits, including enhanced security, decentralization, and transparency, it also raises significant legal and ethical concerns that need to be addressed.

Cyber security Considerations

Block chain's decentralized nature poses unique cyber security challenges. The immutability of block chain transactions makes them attractive targets for cyber attacks, as once recorded, data cannot be altered or removed. Additionally, the anonymity of block chain transactions can facilitate illicit activities such as money laundering and cybercrime.

Vulnerabilities in Block chain Protocols: Block chain protocols are not immune to vulnerabilities that could be exploited by attackers. These vulnerabilities could allow for double-spending attacks, data manipulation, or the theft of private keys.

Smart Contract Security: Smart contracts, self-executing contracts written on the block chain, are particularly vulnerable to security flaws. Errors or vulnerabilities in smart contracts could lead to the loss of funds or the execution of unintended actions.

Regulatory Compliance: Block chain-based applications must comply with applicable cyber security regulations, such as data security laws and anti-money laundering (AML) regulations. Organizations need to implement robust risk

management practices and ensure that their block chain systems meet regulatory requirements.

Legal and Ethical Implications

Beyond cyber security concerns, block chain technology raises a range of legal and ethical issues that need to be carefully considered:

Data Privacy and Ownership: Block chain's inherent transparency and immutability can conflict with individual privacy rights. Organizations need to balance the benefits of block chain with the need to protect personal data and ensure that individuals have control over their information.

Intellectual Property Rights: The ownership and protection of intellectual property (IP) on the block chain can be complex. Clear guidelines are needed to determine how IP rights are established, enforced, and transferred in the block chain ecosystem.

Governance and Regulatory Uncertainty: The decentralized nature of block chain raises questions about governance and regulatory oversight. Governments and regulatory bodies are grappling with how to apply existing laws and regulations to block chain-based applications and how to address emerging issues such as decentralized autonomous organizations (DAOs).

Social and Ethical Impacts: Block chain technology has the potential to disrupt industries, automate processes, and change the way we interact with technology. However, it is crucial to consider the social and ethical implications of these changes, including potential job displacement, algorithmic bias, and the impact on privacy and social norms.

Block chain technology offers immense potential for innovation and transformation in various sectors. However, realizing this potential requires addressing the legal and ethical challenges that arise from its decentralized, transparent, and immutable nature. By fostering collaboration between technology developers, legal experts, policymakers, and ethicists, we can navigate the complexities of block chain technology and harness its power while upholding individual rights, protecting privacy, and promoting responsible innovation.

5.4 CYBER LAWS AND LEGAL AND ETHICAL ASPECTS RELATED TO THE DARKNET AND SOCIAL MEDIA

The darknet, a hidden part of the internet that can only be accessed with specialized software, and social media platforms, which connect billions of people worldwide, have emerged as powerful tools for communication, information sharing, and commerce. However, these platforms also present significant legal and ethical challenges related to cyber security, privacy, and content moderation.

Cyber security Concerns in the Darknet and Social Media

The darknet's anonymity and lack of oversight make it a haven for cybercriminals engaged in activities such as selling illegal goods, trafficking in illicit substances, and conducting cyber attacks. Social media platforms, with their vast user bases and global reach, are also attractive targets for cyber attacks, as they often hold sensitive personal data and are susceptible to the spread of misinformation and malicious content.

Dark net Threats: The dark net poses unique cyber security threats, including:

- **Malware Distribution:** Darknet marketplaces are a breeding ground for malware, where cybercriminals sell malicious software to infect devices and steal data.
- **Data Breaches:** Darknet markets offer services to facilitate data breaches, providing cybercriminals with tools and expertise to steal sensitive information.
- **Cybercrime-as-a-Service (CaaS):** Darknet platforms offer CaaS, providing cybercriminals with access to hacking tools, malware, and even trained personnel to carry out cyber attacks.
- **Social Media Vulnerabilities:** Social media platforms are vulnerable to various cyber attacks, including:
 - **Phishing Attacks:** Social media is a common platform for phishing scams, where attackers attempt to trick users into revealing sensitive information.
 - **Social Engineering:** Cybercriminals use social engineering tactics to manipulate users into disclosing personal information or taking actions that compromise their security.

- **Malicious Links and Content:** Social media platforms are often used to spread malicious links and content that can infect devices with malware or trick users into revealing sensitive information.

Legal and Ethical Implications

The darknet and social media raise a range of legal and ethical issues, including:

Privacy and Surveillance: The anonymity of the darknet and the vast amount of personal data collected by social media platforms raise concerns about individual privacy and the potential for surveillance.

Content Moderation and Freedom of Speech: Balancing content moderation and freedom of speech is a complex challenge for social media platforms. Removing illegal or harmful content is necessary, but it can also lead to censorship and infringe upon freedom of expression.

Accountability and Liability: Determining who is accountable for cyber attacks and illegal activities conducted on the darknet and social media platforms can be challenging.

Misinformation and Disinformation: The spread of misinformation and disinformation on social media platforms poses a threat to democracy, public health, and social stability.

The darknet and social media platforms are powerful tools that offer immense potential for communication, information sharing, and commerce. However, their anonymity, global reach, and vast amount of user data also create significant legal and ethical challenges. Addressing these challenges requires a multifaceted approach involving law enforcement agencies, technology companies, policymakers, and individuals. By fostering collaboration and promoting responsible use of these platforms, we can harness their benefits while mitigating their risks and safeguarding individual rights, privacy, and ethical principles.

5.5 CYBER LAWS OF OTHER COUNTRIES

There are 7 billion people in this world. Approx 65.6 percent% are internet users, that is 4.6 billion people on the internet. And the number just keeps increasing day by day.

Cyber law, also known as Internet Law or Cyber Law, is part of the overall legal system that is related to legal informatics and supervises the digital circulation of information, e-commerce, software, and information security. It is associated with legal informatics and electronic elements, including information systems, computers, software, and hardware. It covers many areas, such as access to and usage of the Internet, encompassing various subtopics, freedom of expression, and online privacy.

Cyber laws help to prevent people from cybercriminals on a small and large scale both with the help of protecting information access from unauthorized people, freedom of speech related to the use of the Internet, privacy, communications, email, websites, intellectual property, hardware, and software, such as data storage devices. As Internet traffic is increasing rapidly day by day, that has led to a higher percentage of legal issues worldwide. Because cyber laws are different according to the country and jurisdiction, restitution ranges from fines to imprisonment, and enforcement is challenging.

Cyber law in USA (United States of America)

The USA is known as a superpower but It has been the top affected country of the world in terms of internet-related crimes.

CFFA (Computer Fraud and Abuse Act) The Computer Fraud and Abuse Act (CFAA) was enacted in 1986, as an amendment to the first federal computer fraud law, to address hacking. Over the years, it has been amended several times, most recently in 2008, to cover a broad range of conduct far beyond its original intent. The CFAA prohibits intentionally accessing a computer without authorization or in excess of authorization but fails to define what “without authorization” means. With harsh penalty schemes and malleable provisions, it has become a tool ripe for abuse and uses against nearly every aspect of computer activity.

Punishment under CFFA(Computer Fraud and Abuse Act) in the USA.

- If anyone obtained national security information so they will be punished under section (a)(1) for 10 years.
- If anyone accessing a Computer and Obtaining Information illegally so they will be punished under section (a)(2) for 1 to 5 years.

- If someone trespassing in a Government Computer so they will be punished under section (a)(3) for 5 years.
- Try to trafficking in Passwords so they will be punished under section (a)(6) for 1 year.
- if someone accessing a Computer to Defraud and Obtain Value so the person will be punished under section (a)(4) for 5 years.
- if someone intentionally Damaging by Knowing Transmission so the person will be punished under section (a)(5)(A) for 1 to 10 years.
- if someone recklessly Damaging by Intentional Access so the person will be punished (a)(5)(B) for 1 to 5 years.
- if negligently Causing Damage and Loss by Intentional Access so the person will be punished under section (a)(5)© for 1 year.
- Extortion Involving Computers under section (a)(7) for 5 years.
- If someone Attempt and Conspiracy to Commit such an Offense under section (b) for 10 years

Cyber law in India

The Information Technology Act of 2000 and its consequent amendments is the only legislative law governing cyber threats in India. While the law encompasses various crimes such as violation of privacy, identity theft, sending obscene material, child pornography, and cyber-terrorism. It lacks on various fronts such as cyber bullying, forgery, piracy, etc. From penalties of up to two lakhs rupees and imprisonment for a privacy violation. To a fine of up to ten lakhs rupees and up to five years in prison for creating and sharing child pornography. To lifelong imprisonment for cyber terrorism. The laws that India has in place are quite strict but there are still a lot of loopholes to cover.

Cyber law in China

Cybercrime in China is mainly provided in the section: “Crimes of Disturbing Public Order” Article 285,286,287 are three major articles that can relate to cybercrime.

Article 285. Whoever violates state regulations and intrudes into computer systems with information concerning state affairs, construction of defense facilities, and

sophisticated science and technology is to be sentenced to not more than three years of fixed-term imprisonment or criminal detention.

Article 286. Whoever violates states regulations and deletes, alters, adds, and interferes in computer information systems, causing abnormal operations of the systems and grave consequences, is to be sentenced to not more than five years of fixed-term imprisonment or criminal detention; when the consequences are particularly serious, the sentence is to be not less than five years of fixed-term imprisonment.

Whoever violates state regulations and deletes, alters, or adds the data or application programs installed in or processed and transmitted by the computer systems, and causes grave consequences, is to be punished according to the preceding paragraph.

Whoever deliberately creates and propagates computer viruses and other programs which sabotage the normal operation of the computer system and cause grave consequences is to be punished according to the first paragraph.

Article 287. Whoever uses a computer for financial fraud, theft, corruption, misappropriation of public funds, stealing state secrets, or other crimes is to be convicted punished according to relevant regulations of this law.

Cyber laws in Spain

Spain is also a very strict rule related to cybercrimes

1. Any individual who, for the purpose of discovering the secrets or violating the privacy of another and without the consent of the latter takes possession of that individual's papers, letters, electronic mail messages, or any other personal documents or belongings or intercepts his or her telecommunications or uses technical devices for listening, transmitting, recording or reproducing sound or images or any other communications signal, will be punished by imprisonment from between one and four years and a fine of between twelve and twenty-four months

2. The same punishment will be applicable to any individual who, without authorization, seizes, uses, or modifies, to the detriment of a third party, such as private personal or family data of another individual as may be recorded on computer, electronic or telematic files or media, or in any other type of file or record, whether public or private. The same punishment will be imposed on any individual who, without

authority, accesses such data by any means or alters or uses such data to the detriment of the owner of the data or of a third party.

3. Punishment consisting of imprisonment from between two and five years will be imposed if the data or facts discovered or the images captured, as indicated in the preceding paragraphs, are divulged, revealed or transferred to third parties. Punishment consisting of imprisonment from between one and three years and a fine of between twelve and twenty-four months [sic] will be imposed on any individual who, with prior knowledge of the illicit origin of such facts or data but without having taken part in their discovery, commits the acts described in the preceding paragraph.

4. If the acts described in paragraphs 1 and 2 of this article are committed by the persons in charge of or responsibility for the computer, electronic or telemetric files and media or files or records, punishment consisting of imprisonment from between three and five years will be imposed, and if such private data are disseminated, transferred or made public, the upper half of the punishment will be imposed.

5. In addition, when the acts described in the above sections involve personal data revealing the ideology, religion, beliefs, health, racial origin, or sexual orientation, or if the victim is a minor or incapacitated, the upper half of the punishments stipulated will be imposed.

6. If such acts are committed with intent to profit, the upper half [sic] of the punishments set forth respectively in paragraphs 1 through 4 of this article will be imposed. If in addition, they involve the data mentioned in paragraph

7. The punishment will consist of imprisonment from between four and seven years.

5.6 THE INFORMATION TECHNOLOGY ACT, 2000 (IT ACT)

The Information Technology Act, 2000 (IT Act) is a landmark legislation in India that governs the use of electronic data interchange and other means of communication through electronic means. It was enacted in 2000 and has been amended several times since then to keep pace with the evolving technological landscape.

Objectives of the IT Act

The IT Act aims to:

Provide legal recognition for electronic transactions and contracts

Facilitate electronic filing of documents with government agencies

Protect electronic records and digital signatures

Prevent cybercrimes and punish offenders

Establish a cybercrime adjudication mechanism

Major Amendments to the IT Act

Since its inception, the IT Act has undergone several amendments to address emerging technological advancements and address new challenges. Here are some of the major amendments:

IT Act Amendment 2002: This amendment introduced the concept of electronic security practices and penal provisions for cybercrimes.

IT Act Amendment 2008: This amendment introduced the controversial Section 66A, which penalized sending "offensive messages," and Section 69, which gave authorities the power of "interception or monitoring or decryption of any information through any computer resource."

IT Act Amendment 2016: This amendment introduced the concept of "data fiduciaries" and established a framework for data protection and privacy.

Significance of the IT Act

The IT Act plays a crucial role in regulating the digital space and ensuring cyber security in India. It has been instrumental in:

Facilitating the growth of e-commerce and electronic transactions

Providing a legal framework for electronic governance initiatives

Combating cybercrimes and protecting individuals from online harm

Promoting data protection and privacy in the digital age

Challenges and Future Directions

While the IT Act has been a valuable piece of legislation, it faces certain challenges in keeping pace with the rapid advancements in technology. Some of the areas that require further consideration include:

Addressing the growing concerns about data privacy and the use of personal data in the digital economy

Regulating the use of social media and emerging technologies like artificial intelligence and machine learning

Strengthening the framework for cybercrime prevention and investigation

The IT Act has played a pivotal role in shaping India's digital landscape and ensuring cyber security. As technology continues to evolve, it is imperative to adapt and refine the IT Act to address emerging challenges and protect the rights of individuals in the digital age.

5.7 LIMITATIONS OF IT ACT 2000 IN INDIA

The Information Technology Act, 2000 (IT Act) is a landmark legislation in India that governs the use of electronic communication and commerce. While it has been instrumental in facilitating the growth of the internet and e-commerce in India, the IT Act also has certain limitations that have been identified over the years.

Key limitations of the IT Act, 2000:

Scope and Coverage: The IT Act focuses primarily on electronic transactions and offenses committed within the cyberspace. It does not adequately address broader cybercrime issues such as cyber attacks on critical infrastructure, cyber espionage, and online child sexual abuse.

Data Protection and Privacy: The IT Act lacks a comprehensive data protection framework. While it provides some basic safeguards for personal data, it does not fully address the growing concerns over data privacy and the misuse of personal information.

Cybercrime Investigation and Prosecution: The IT Act's provisions for cybercrime investigation and prosecution are often criticized for being outdated and

ineffective. The lack of specialized cybercrime units and trained personnel hinders the timely and effective investigation and prosecution of cybercrimes.

Interception and Surveillance: The IT Act grants the government powers to intercept and monitor electronic communications in certain circumstances. However, these powers are susceptible to abuse and lack adequate safeguards to protect privacy rights.

Harmonization with International Standards: The IT Act's provisions may not align with international standards and best practices in cybersecurity and data protection. This can create challenges for cross-border cooperation and data exchange.

Addressing the Limitations:

To address these limitations, the Indian government has undertaken several initiatives, including:

Amendments to the IT Act: The IT Act has been amended several times to incorporate new technologies and address emerging cybercrime threats. However, further amendments are needed to address the gaps in data protection, cybercrime investigation, and interception powers.

Data Protection Bill: The government is working on a comprehensive data protection bill that aims to establish a robust framework for data privacy and protection. The bill is expected to address concerns over personal data collection, usage, and storage.

Cyber security Policy: The government has adopted a national cyber security policy that outlines a multi-pronged approach to cyber security, including strengthening cyber infrastructure, enhancing cybercrime investigation capabilities, and promoting cyber security awareness.

International Cooperation: India is actively engaged in international cooperation efforts to combat cybercrime and promote cyber security. It participates in various multilateral forums and agreements to share information, expertise, and best practices.

Despite the limitations, the IT Act, 2000, has played a significant role in shaping India's digital landscape. Ongoing efforts to address the limitations and strengthen

cyber security measures will be crucial in ensuring a secure and trusted digital environment for India's citizens and businesses.

5.8 RIGHT TO INFORMATION ACT

Definition of 'Right To Information'

RTI (Right to information) is an act aimed to ensure transparency and accountability in the governance of the country. Under the Right to Information, people have the deserved authority to question various government programs and the government is expected to answer the questions. Any Indian citizen can file an RTI, without any legal help. Its a very simple procedure. Tamil Nadu was the first state to implement Freedom of Information Act, 1997 and Rajasthan was the first state to officially pass the RTI in the year 2000.

This act was passed in 2005 in the Parliament, meaning now it was applicable to all states of India.

According to Section 2 (f), "information" means any material in any form including records, documents, memos, e-mails, opinions, advices, press releases, circulars, orders, logbooks, contracts, reports, papers, samples, models, data material held in any electronic form and information relating to any private body which can be accessed by a public authority under any other law for the time being in force

- A citizen has a right to obtained any- records, documents, memos, e-mails, opinions, advices, press releases, circulars, orders, logbooks, contracts, reports, papers, samples, models, data material held in any electronic form and information relating to any private body, from any public authority, which is held by a public authority or which is held under its control.
- A citizen has a right to see a work document or record closely, carefully and purposefully.
- A citizen has a right noting down certain information from the documents inspected.
- A citizen has a right to take samples from the material being purchased or used by the Public Authorities.
- A citizen has a right to obtained information in the form of diskettes, floppies, tapes, video cassettes or in any other electronic mode or through printouts where such information is stored in computer or in any other device.

- A citizen has no right to obtain information from other than public authority i.e. from private body, institution or organization including NGO's which are self-financed. However it is not included in the definition but noteworthy to mention here, that:
- The Act gives the right to information only to the citizens of India. It does not make provision for giving information to Corporations, Associations, Companies etc. which are legal entities/persons, but not citizens.
- Under the Act only such information is required to be supplied, which already exists and is held by the public authority or held under the control of the public authority.
- Right to information is not absolute. Section 8 and 9 provided the provisions about the information which are exempted for disclosure.
- Right to information is the fundamental right of every citizen
- Right to information is implicitly guaranteed by the constitution
- The Act is a big step towards making the citizens informed about the activities of the Government
- The act provided a machinery setup for access to information held by and under the control of every public authority.
- The term information include records, documents, memos, e-mails, opinions, advices, press releases, contracts, reports, papers, samples, models, and any other material produced by a computer or any other device;
- Information relating to any private body which can be accessed by a public authority under any other law for the time being in force, is also accessible.
- Right to information also covers inspection of records, documents etc. Taking notes from them and also taking certified samples of material.
- Every public authority is obliged under the provisions of Act to provide information on request whether written or by electronics means, except which are explicitly prohibited by the act.
- There is also provision of penalty for not providing information to the requester.
- Central information Commission is to be constituted under Central Government and State Information Commission are to be constituted in every state
- RTI puts power directly into the hands of the common people. It becomes a powerful tool against the prevailing corruption in India.

- The Act ensure that the records are duly catalogued and indexed in such a manner and form that it may facilitate the right to information.
- After the end of each year, Commission, are required to prepare reports on the implementation of the provisions of the Act during that year.

5.9. RTI AS A REPORTING TOOL. EXPLAIN

The Right to Information (RTI) Act, 2005, is a powerful tool that can be used as a reporting tool for various purposes. It empowers citizens to access information held by public authorities, enabling them to hold the government accountable, promote transparency, and expose corruption.

1. Investigating Public Issues: RTI can be used to investigate public issues and uncover hidden information. Journalists and activists often use RTI to gather data and evidence for their investigations. For instance, RTI requests have been used to expose corruption in government projects, uncover irregularities in public procurement, and shed light on human rights abuses.

2. Monitoring Government Programs and Schemes: RTI can be used to monitor the implementation of government programs and schemes. Citizens can file RTI requests to obtain information on the allocation of funds, the progress of projects, and the utilization of resources. This helps ensure that government programs are functioning effectively and delivering the intended benefits.

3. Tracking Public Funds and Resources: RTI can be used to track the flow of public funds and resources. Citizens can file RTI requests to obtain information on the expenditure of government departments, the allocation of budgetary resources, and the utilization of public assets. This helps ensure that public funds are being used for the intended purposes and not for personal gain.

4. Promoting Transparency and Accountability: RTI promotes transparency and accountability in governance by making government information accessible to the public. Citizens can use RTI to hold their elected representatives and public officials accountable for their actions and decisions. This leads to better governance and increased trust in public institutions.

5. Exposing Corruption and Maladministration: RTI can be used to expose corruption and maladministration in government offices. Citizens can file RTI requests

to obtain information on irregularities, misuse of power, and non-compliance with rules and regulations. This helps bring corrupt officials to justice and deter future misconduct.

6. Empowering Citizens and Grassroots Movements: RTI empowers citizens to participate in governance and hold their government accountable. Grassroots movements and civil society organizations can use RTI to advocate for their rights, demand reforms, and promote social justice.

7. Strengthening Democracy: RTI strengthens democracy by promoting transparency, accountability, and citizen participation in governance. It empowers citizens to hold their government accountable, ensures the rule of law, and protects fundamental rights.

In conclusion, RTI is a powerful tool for reporting, investigating, and promoting transparency in governance. It empowers citizens to hold their government accountable, expose corruption, and ensure that public funds are used for the intended purposes. RTI is a valuable tool for journalists, activists, and citizens alike, and it plays a crucial role in strengthening democracy and ensuring good governance.

5.10 MEDIA AND PRIVACY IN THE DIGITAL AGE

In the ever-evolving digital landscape, the relationship between media and privacy has become increasingly complex and fraught with challenges. The pervasiveness of technology and the insatiable appetite for information have blurred the lines between public and private spheres, leaving individuals vulnerable to the scrutinizing gaze of the media. This essay will explore the intricate dynamics between media and privacy, examining the threats posed by media intrusion and the urgent need for robust privacy protections.

The Threat of Media Intrusion

The media's relentless pursuit of newsworthy content has often come at the expense of individual privacy. The relentless paparazzi culture, the proliferation of social media, and the advancement of surveillance technologies have created an environment where privacy is constantly under siege. The media's ability to capture and disseminate intimate details of individuals' lives, often without their consent or

knowledge, has raised serious concerns about the erosion of personal autonomy and dignity.

The Chilling Effect on Personal Expression

The fear of media intrusion can have a chilling effect on personal expression and freedom of association. Individuals may self-censor their behavior and opinions, fearing that their privacy will be violated and their lives exposed to public scrutiny. This self-censorship can stifle open discourse and limit the exchange of ideas, ultimately hindering the fundamental right to freedom of expression.

The Need for Robust Privacy Protections

The delicate balance between media freedom and individual privacy requires a nuanced approach to privacy protection. While upholding the media's right to inform and scrutinize, it is equally important to safeguard individuals' right to privacy and control over their personal information. Robust privacy protections should include:

- Stricter laws against unauthorized surveillance and data collection
- Clear and enforceable privacy policies by media organizations
- Enhanced transparency and accountability in media practices
- Empowerment of individuals to control their personal information

The relationship between media and privacy is a complex and evolving one, demanding a delicate balance between the media's right to inform and individuals' right to privacy. In a world where privacy is constantly under threat, it is imperative to strengthen privacy protections and foster a culture of respect for individual autonomy. Only then can we ensure that the media's role as a cornerstone of democracy is not achieved at the expense of fundamental human rights.

5.11 PRIVACY BILL IN INDIA AND IN OTHER COUNTRIES.

The Personal Data Protection Bill, 2022 (PDPB), is a proposed Indian legislation that aims to regulate the collection, storage, and use of personal data by organizations. The Bill is currently under consideration by the Indian Parliament and is expected to be passed soon.

Key Features of the PDPB

The PDPB has several key features that aim to protect the privacy of Indian citizens. These features include: A definition of personal data that is broad enough to cover all types of personal information, including sensitive personal data.

- A requirement for organizations to obtain explicit consent from individuals before collecting their personal data.
- A requirement for organizations to be transparent about how they collect, use, store, and share personal data.
- A right for individuals to access, rectify, erase, restrict, and object to the processing of their personal data.
- A requirement for organizations to appoint data protection officers (DPOs) to oversee their compliance with the PDPB.

International Comparisons

The PDPB is similar to data protection laws in other countries, such as the General Data Protection Regulation (GDPR) in the European Union and the California Consumer Privacy Act (CCPA) in the United States. However, there are some key differences between the PDPB and these other laws.

For example, the PDPB does not have a comprehensive right to data portability, which allows individuals to easily transfer their personal data from one organization to another. Additionally, the PDPB does not have a specific provision for data localization, which requires that personal data be stored within the country where it is collected.

The PDPB is a significant step forward for data protection in India. The Bill is expected to have a profound impact on the way organizations collect, store, and use personal data in India.

Other Countries

In addition to India, several other countries have also enacted data protection laws in recent years. These countries include:

- Australia: The Privacy Act 1988
- Brazil: General Law for the Protection of Personal Data (LGPD)
- Canada: Personal Information Protection and Electronic Documents Act (PIPEDA)
- China: Personal Information Protection Law (PIPL)

- Japan: Act on Protection of Personal Information (APPI)
- South Korea: Personal Information Protection Act (PIPA)
- United Kingdom: Data Protection Act 2018

These laws vary in their scope and requirements, but they all aim to protect the privacy of individuals and give them control over their personal data.

The right to data privacy is a fundamental human right that empowers individuals to control the collection, use, and disclosure of their personal information. It encompasses the right to be free from unwarranted surveillance and the right to access, rectify, and erase personal data that is held by others.

5.12 RIGHT TO DATA PRIVACY

Data privacy is essential for protecting individuals' autonomy, dignity, and freedom of expression. In today's digital age, where vast amounts of personal data are collected and stored, it is crucial to safeguard individuals' rights and prevent the misuse of their data.

Importance of Data Privacy

Threats to Data Privacy: The increasing collection and use of personal data pose significant threats to data privacy. These threats include:

Unwarranted surveillance: Governments and private companies are increasingly collecting personal data through various means, such as facial recognition technology, social media tracking, and location data tracking. This raises concerns about the potential for mass surveillance and the erosion of individuals' privacy.

Data breaches: Personal data is often stored in centralized databases, making it vulnerable to data breaches. These breaches can expose sensitive information, such as financial records, medical records, and social security numbers, leading to identity theft, financial fraud, and other harm.

Misuse of personal data: Personal data can be used for purposes that individuals did not consent to or may not be aware of. This includes profiling individuals for targeted advertising, manipulating their behaviour, and making discriminatory decisions based on their data.

Protecting Data Privacy

Several measures can be taken to protect data privacy. These measures include:

Strong data protection laws: Governments should enact and enforce strong data protection laws that give individuals control over their personal data and require organizations to collect, use, and store personal data responsibly.

Data minimization: Organizations should only collect the personal data that is necessary for the purpose specified and should not retain it for longer than necessary.

Transparency: Organizations should be transparent about their data collection practices and should provide individuals with clear and concise information about how their data is being used.

Security: Organizations should implement appropriate security measures to protect personal data from unauthorized access, use, disclosure, alteration, or destruction.

Individual empowerment: Individuals should be empowered to access, rectify, erase, and restrict the processing of their personal data. They should also be able to lodge complaints about the misuse of their data.

Data privacy is a critical issue in today's digital world. By strengthening data protection laws, promoting data minimization practices, enhancing transparency, implementing robust security measures, and empowering individuals, we can protect the right to data privacy, safeguard individual autonomy, and foster a more secure and trustworthy digital environment.

5.13 RELEVANT SECTIONS OF THE IT ACT

The Information Technology Act, 2000, is a landmark legislation in India that deals with cybercrime and e-commerce. It has been amended several times since it was first enacted, and it now covers a wide range of offenses, including hacking, identity theft, and online fraud.

Here are some of the most relevant sections of the IT Act:

Section 66A: This section deals with the punishment for sending offensive messages through communication service, etc. It states that any person who sends by any means of a computer communication a message which is grossly offensive or menacing in character shall be punishable with imprisonment for a term which may extend to two years, and with fine.

Section 66B: This section deals with the punishment for dishonestly receiving stolen computer resource or communication device. It states that any person who dishonestly receives or retains the possession of a stolen computer resource or communication device, knowing it to be stolen, shall be punishable with imprisonment for a term which may extend to three years, or with fine, or with both.

Section 66C: This section deals with the punishment for identity theft. It states that any person who, having any reason to believe that a particular electronic record or digital signature is forged or falsely made, knowingly transmits or causes it to be transmitted in any electronic form, shall be punishable with imprisonment for a term which may extend to three years, and with fine which may extend to two lakhs rupees.

Section 66D: This section deals with the punishment for cheating by personation by using computer resource. It states that any person who cheats by personation using computer resource shall be punishable with imprisonment for a term which may extend to one year, or with fine which may extend to one lakhs rupees, or with both.

Section 66E: This section deals with the punishment for violation of privacy. It states that any person who, without the consent of the person concerned, knowingly discloses or transmits any sensitive personal information about another person without his or her consent, shall be punishable with imprisonment for a term which may extend to two years, or with fine which may extend to two lakhs rupees, or with both.

These are just a few of the many relevant sections of the IT Act. The Act is a complex piece of legislation, and it is important to seek legal advice if you are unsure about your rights or obligations under the Act.

5.14 SECTION 43A AND SECTION 72 A.

India does not have a comprehensive legislation for the protection of privacy of an individual. Article 21 of the Constitution of India has been extended to include the right to privacy as a fundamental right available under the Constitution. However, being a fundamental right, it can only be enforced only against the State. The legal framework in India with respect to the enforcement of the right to privacy of an individual against other individuals is still in its nascent stage.

In today's knowledge based society where data is critical and easily accessible to everyone, it becomes even more pertinent to have privacy and data protection laws

in place to counter the increasing risk of misuse of personal data. Various initiatives have been taken in this regard by the government as well as certain NGOs. The Centre for Internet and Society, a NGO, had also submitted a citizens' draft of the Privacy (Protection) Bill, 2013 majorly outlining law in relation to data protection, interception and surveillance.

A draft bill on the Right to Privacy was prepared by the Ministry of Personnel, Public Grievance and Pensions and the Department of Personnel and Training and submitted to the Cabinet in 2011. Despite multiple discussions on the draft bill, the same was never enacted. A Committee was also set up by the Planning Commission to deliberate and provide suggestions for a proposed Privacy Act in India. The Committee, chaired by Justice A. P. Shah, submitted its report in 2012. The Committee was of the opinion that "any proposed framework for privacy legislation must be technologically neutral and inter operable with international standards."

The Law as it stands

The law relating to data protection and privacy in India as prevailing today is encompassed in the Information Technology Act, 2000 ("Act") and the rules made thereunder. A brief synopsis of the extant law in this regard is provided below:

Protection under the Act

The Act extends penalty for the breach of privacy and confidentiality. However, up till 2008, this remedy was available only against persons who were conferred under the Act, secured access to any electronic record, book, register, correspondence, information, document or material without the consent of the persons concerned, and such person has disclosed the material. Thus, this remedy had a limited scope and was not concerned with the protection of data in a private transaction.

This deficiency was cured to some extent vide the Information Technology (Amendment) Act, 2008 which, among other things also extended certain protections to the right to privacy. Section 43A and Section 72A imposed liability to compensate for failure to protect data, and punishment for the disclosure of information in breach of a contract respectively. While Section 43A was enforceable only against body corporates, i.e. any enterprise engaged in commercial or professional activities, including any company, firm, sole proprietorship or any other association of persons,

Section 72A provided remedy against any person for a breach of privacy/confidentiality pursuant to a lawful contract.

The Act, vide Section 43A and 72A provide for remedies in case of breach of privacy and confidentiality as detailed below:

Section 43A – Compensation for Failure to Protect Data

Body corporates are liable to compensate any person who is affected as a result of their negligence in maintaining ‘reasonable security practices and procedures’, thereby causing any wrongful gain or wrongful loss to any person. Reasonable security practices and procedures would mean such practices and procedures to protect the unauthorized access, use, damage, etc. of any sensitive personal data[1] and information as agreed between the parties. Where no such agreement exists between parties, it would mean such practices and procedures as prescribed by law[2]. A body corporate shall become liable if it was negligent in maintaining any sensitive personal data or information that it possesses, deals or handles with in a computer resource which it owns controls or operates.

Section 72 – Penalty For Breach of Confidentiality and Privacy

The Act has conferred powers on the following persons to have access to the computer and data without any consent of the persons concerned:

Controller of Certifying Authority, or

Any person authorized by the Controller to exercise such power.

Any person authorized by the appropriate government to access the protected system.

The operational staff of the Certifying Authority (only on a ‘need-to-know’ basis)

This Section is applicable only to the above mentioned persons. A penalty that may extend up to Rs. 1,00,000/- (Rupees One Lakhs) and/or imprisonment which may extend to 2 (two) years shall be imposed on such persons for disclosing the material that they have secured access to.

Section 72A – Disclosure of Information in Breach of Lawful Contract

This provision makes it an offence to disclose any material containing personal information about another person without the consent of the person concerned or in

breach of a lawful contract, with the intention or knowledge that it is likely to cause wrongful gain or wrongful loss. Any person who is guilty of such disclosure shall be punished with imprisonment for a term which may extend to 3 (three) years and/or imposed with a fine that may extend to Rs. 5,00,000/- (Rupees Five Lakhs). It may be noted that the liability under this provision is also extended to any such person who on behalf of another receives, stores or transmits an electronic record^[3] or provides any service with respect to any electronic record such as network service providers, web-hosting service providers, search engines, online payment sites, etc. (“intermediary”). The primary difference between Section 72 and Section 72A is their applicability – Section 72 can be enforced against the lawful authority, while 72A is enforceable against any person who discloses the information in breach of a lawful contract or without the consent of the person concerned. It is interesting that the penalty for unauthorized disclosure by private persons is greater than penalty for unauthorized disclosure by lawful authority.

Our next post outlines the right to privacy in respect of data protection as provided under the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, are a set of regulations in India that govern the collection, storage, use, and disclosure of sensitive personal data or information. The Rules were issued by the Ministry of Information Technology (MeitY) under the Information Technology Act, 2000.

5.15 SENSITIVE PERSONAL DATA OR INFORMATION RULES (SPDI)

SPDI is defined as any personal information that may reveal racial or tribal origin, political opinions, religious or philosophical beliefs, sexual orientation, membership of unions, associations or organizations, biometric information, and any detail relating to the above clauses as provided to a body corporate for providing service; and any of the information received under above clauses by a body corporate for processing, stored or processed under lawful contract or otherwise.

The Rules require body corporates that possess, deal or handle SPDI to implement and maintain reasonable security practices and procedures to protect such

data from unauthorized access, use, disclosure, alteration, or destruction. Some of the specific requirements include:

Appointment of a data security officer: Body corporate that process SPDI are required to appoint a data security officer who is responsible for overseeing the implementation and maintenance of security practices and procedures.

Collection and storage of SPDI: SPDI can only be collected with the consent of the individual to whom it relates. The Rules also specify that SPDI must be stored in a secure manner to prevent unauthorized access.

Disclosure of SPDI: Body corporates can only disclose SPDI to third parties with the consent of the individual to whom it relates. However, there are some exceptions to this rule, such as when disclosure is necessary for compliance with a law or for preventing harm to an individual.

Disposal of SPDI: SPDI must be disposed of in a secure manner when it is no longer required.

Penalties for non-compliance

Body corporate that fail to comply with the Rules may be liable for a fine of up to two lakhs rupees. Additionally, body corporate may be liable for compensation to individuals who have suffered loss or damage as a result of the body corporate failure to comply with the Rules.

Impact of the Rules

The Rules have had a significant impact on data protection in India. They have raised awareness of the importance of data privacy and have encouraged body corporate to implement stronger security measures to protect SPDI. The Rules have also been instrumental in promoting transparency and accountability in the handling of SPDI.

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, are an important piece of legislation that provides a framework for the protection of sensitive personal data in India. The Rules have helped to raise awareness of data privacy issues and have encouraged body corporates to implement stronger security measures. The Rules have

also played a role in promoting transparency and accountability in the handling of SPDI.

5.16 PERSONAL DATA PROTECTION BILL, 2019

The Personal Data Protection Bill, 2019 was introduced in Lok Sabha by the Minister of Electronics and Information Technology, Mr. Ravi Shankar Prasad, on December 11, 2019. The Bill seeks to provide for protection of personal data of individuals, and establishes a Data Protection Authority for the same.

Applicability: The Bill governs the processing of personal data by: (i) government, (ii) companies incorporated in India, and (iii) foreign companies dealing with personal data of individuals in India. Personal data is data which pertains to characteristics, traits or attributes of identity, which can be used to identify an individual. The Bill categorises certain personal data as sensitive personal data. This includes financial data, biometric data, caste, religious or political beliefs, or any other category of data specified by the government, in consultation with the Authority and the concerned sectional regulator.

Obligations of data fiduciary: A data fiduciary is an entity or individual who decides the means and purpose of processing personal data. Such processing will be subject to certain purpose, collection and storage limitations. For instance, personal data can be processed only for specific, clear and lawful purpose. Additionally, all data fiduciaries must undertake certain transparency and accountability measures such as: (i) implementing security safeguards (such as data encryption and preventing misuse of data), and (ii) instituting grievance redressal mechanisms to address complaints of individuals. They must also institute mechanisms for age verification and parental consent when processing sensitive personal data of children.

Rights of the individual: The Bill sets out certain rights of the individual (or data principal). These include the right to: (i) obtain confirmation from the fiduciary on whether their personal data has been processed, (ii) seek correction of inaccurate, incomplete, or out-of-date personal data, (iii) have personal data transferred to any other data fiduciary in certain circumstances, and (iv) restrict continuing disclosure of their personal data by a fiduciary, if it is no longer necessary or consent is withdrawn.

Grounds for processing personal data: The Bill allows processing of data by fiduciaries only if consent is provided by the individual. However, in certain

circumstances, personal data can be processed without consent. These include: (i) if required by the State for providing benefits to the individual, (ii) legal proceedings, (iii) to respond to a medical emergency.

Social media intermediaries: The Bill defines these to include intermediaries which enable online interaction between users and allow for sharing of information. All such intermediaries which have users above a notified threshold, and whose actions can impact electoral democracy or public order, have certain obligations, which include providing a voluntary user verification mechanism for users in India.

Data Protection Authority: The Bill sets up a Data Protection Authority which may: (i) take steps to protect interests of individuals, (ii) prevent misuse of personal data, and (iii) ensure compliance with the Bill. It will consist of a chairperson and six members, with at least 10 years' expertise in the field of data protection and information technology. Orders of the Authority can be appealed to an Appellate Tribunal. Appeals from the Tribunal will go to the Supreme Court.

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

Exemptions: The central government can exempt any of its agencies from the provisions of the Act: (i) in interest of security of state, public order, sovereignty and integrity of India and friendly relations with foreign states, and (ii) for preventing incitement to commission of any cognisable offence (i.e. arrest without warrant) relating to the above matters. Processing of personal data is also exempted from provisions of the Bill for certain other purposes such as: (i) prevention, investigation, or prosecution of any offence, or (ii) personal, domestic, or (iii) journalistic purposes. However, such processing must be for a specific, clear and lawful purpose, with certain security safeguards.

Offences: Offences under the Bill include: (i) processing or transferring personal data in violation of the Bill, punishable with a fine of Rs 15 crore or 4% of the annual turnover of the fiduciary, whichever is higher, and (ii) failure to conduct a data audit, punishable with a fine of five crore rupees or 2% of the annual turnover of the fiduciary,

whichever is higher. Re-identification and processing of de-identified personal data without consent is punishable with imprisonment of up to three years, or fine, or both.

Sharing of non-personal data with government: The central government may direct data fiduciaries to provide it with any: (i) non-personal data and (ii) anonymised personal data (where it is not possible to identify data principal) for better targeting of services.

Amendments to other laws: The Bill amends the Information Technology Act, 2000 to delete the provisions related to compensation payable by companies for failure to protect personal data.

5.17 THE RIGHT TO BE FORGOTTEN

The right to be forgotten "reflects the claim of an individual to have certain data deleted so that third persons can no longer trace them". It has been defined as "the right to silence on past events in life that are no longer occurring".

The right to be forgotten, also known as the right to erasure, is a legal concept that allows individuals to request the removal of their personal data from the internet. This right is based on the idea that individuals have the right to control their own personal information and to have it removed from public view if it is no longer relevant or if it is causing them harm.

The right to be forgotten was first established in the European Union in 2014 with the passage of the General Data Protection Regulation (GDPR). The GDPR grants individuals a number of rights regarding their personal data, including the right to access, rectify, and erase their data. The right to be forgotten is a specific application of the right to erasure, and it applies to personal data that is no longer necessary for the purposes for which it was collected or processed.

The right to be forgotten has been a controversial topic since its inception. Proponents of the right argue that it is essential for protecting individual privacy and preventing harm from the ongoing availability of personal data. Opponents of the right argue that it is a threat to freedom of expression and that it could be used to suppress legitimate information.

Despite the controversy, the right to be forgotten has been upheld by courts in a number of cases. In 2014, the European Court of Justice ruled that Google had a legal

obligation to remove links to a Spanish newspaper article about a man's foreclosure case. The Court found that the article was no longer relevant and that the man's right to privacy outweighed the public's right to access the information.

The right to be forgotten is a complex and evolving issue. It is likely to continue to be debated in courts and legislatures around the world.

Who can exercise the right to be forgotten? The right to be forgotten can be exercised by any individual whose personal data is processed by an organization. This includes data that is processed on the internet, as well as data that is stored in other forms, such as in databases or files.

What information can be removed under the right to be forgotten?

The right to be forgotten applies to a wide range of personal data, including:

Information that is no longer necessary for the purposes for which it was collected or processed

- Information that is inaccurate or incomplete
- Information that is excessive or irrelevant
- Information that is causing the individual harm
- When will a request for erasure be denied?
- A request for erasure will be denied if:
 - The information is necessary for the purposes of freedom of expression and information
 - The information is necessary for the execution of a legal obligation
 - The information is necessary for the establishment, exercise, or defense of legal claims
 - The information is necessary for the protection of the interests of another person

How can exercise the right to be forgotten?

To exercise the right to be forgotten, contact the organization that is processing your personal data by sending a written request to the organization's data protection officer. The request should include:

- The name and contact details
- The specific information you want to be removed

- The reasons why you want to have the information removed
- Any supporting documentation, such as copies of court orders or legal agreements

The organization will have a month to review your request and respond . If the organization denies the request, can appeal the decision to the supervisory authority in the country.

The right to be forgotten is a complex and evolving issue. It is important to seek legal advice if you are considering exercising this right.

5.18 THE EU'S DIGITAL SERVICES ACT (DSA)

The EU's Digital Services Act (DSA) is a landmark piece of legislation that aims to regulate online platforms and services. The DSA was adopted in July 2022 and came into force on November 16, 2023.

The DSA is a comprehensive piece of legislation that covers a wide range of issues, including:

- **Illegal content:** The DSA requires online platforms to take measures to remove illegal content, such as hate speech, terrorist content, and child sexual abuse material.
- **Harmful content:** The DSA also requires online platforms to take measures to address the spread of harmful content, such as disinformation and misinformation.
- **Transparency and accountability:** The DSA requires online platforms to be more transparent about their algorithms and how they moderate content. It also requires them to be more accountable for their actions.
- **Protections for users:** The DSA includes a number of protections for users, such as the right to appeal decisions made by online platforms and the right to access their personal data.

The DSA is a major step forward in the regulation of online platforms. It is a complex and ambitious piece of legislation, and it is likely to have a significant impact on the way that online platforms operate.

Key Challenges and Debates.(EU's Digital Services Act, 2023)

The EU's Digital Services Act (DSA) is a landmark piece of legislation that aims to regulate online platforms and services. The DSA was adopted in July 2022 and came into force on November 16, 2023.

Key Challenges

The DSA is a complex and ambitious piece of legislation, and it faces several key challenges in its implementation:

Scope and Definition: Determining the exact scope of the DSA and defining key terms like "illegal content" and "harmful content" is crucial. This is essential to ensure that the DSA is applied effectively and fairly to all relevant platforms and services.

Balance and Proportionality: Striking the right balance between regulating online platforms and protecting freedom of expression is a delicate task. The DSA must ensure that it safeguards users from harmful content without unduly restricting legitimate expression and innovation.

Enforcement and Oversight: Enforcing the DSA across the EU and ensuring consistent oversight by national authorities is critical. This requires strong coordination and cooperation among member states, as well as adequate resources and expertise.

Adaptability and Future-Proofing: The DSA needs to be adaptable to the ever-evolving digital landscape and emerging technologies. It should incorporate mechanisms for regular review and updates to remain relevant and effective.

Key Debates

The DSA has sparked several ongoing debates regarding its implementation and potential implications:

Platform Responsibilities: The extent of platforms' responsibilities in identifying, removing, and preventing the spread of illegal and harmful content is a subject of debate. Some argue for stricter liability, while others emphasize the need for proportionate measures and due process.

Algorithmic Transparency and Accountability: The DSA mandates greater transparency and accountability for platform algorithms. However, defining the level of detail required and ensuring meaningful transparency without compromising proprietary information and innovation are ongoing challenges.

User Empowerment and Protection: Balancing user empowerment with platform oversight is crucial. The DSA aims to empower users with more control over their online experiences, but it must also ensure that users are adequately protected from harm.

Global Implications and Interoperability: The DSA's impact extends beyond the EU, as it affects global platforms and services. Ensuring interoperability with other regulatory frameworks and fostering international cooperation are essential for effective global regulation.

Check your progress

1. SPDI
2. The Computer Fraud and Abuse Act (CFAA) was enacted in 1986.
3. Darknet marketplaces are a breeding ground for -----.
4. Social media platforms are often used to spread ----- links and content that can infect devices

Glossaries

Data minimization: Organizations should only collect the personal data that is necessary for the purpose specified and should not retain it for longer than necessary.

Data privacy is a critical issue in today's digital world. By strengthening data protection laws, promoting data minimization practices, enhancing transparency, implementing robust security measures, and empowering individuals, we can protect the right to data privacy, safeguard individual autonomy, and foster a more secure and trustworthy digital environment.

Security: Organizations should implement appropriate security measures to protect personal data from unauthorized access, use, disclosure, alteration, or destruction.

Misuse of personal data: Personal data can be used for purposes that individuals did not consent to or may not be aware of. This includes profiling individuals for targeted advertising, manipulating their behaviour, and making discriminatory decisions based on their data.

Check your answer

1. Sensitive Personal Data or Information rules
2. 1986
3. malware
4. Malicious

Suggested Readings

<https://ayyucekizrak.gitbook.io/computers-and-ethics-lecturenotes/computers-and-ethics/computers-and-ethics-lecture-notes/7.-legal-aspects-of-iot>

<https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023>

<https://em360tech.com/tech-article/navigating-legal-and-ethical-issues-ai-enterprise-cybersecurity>