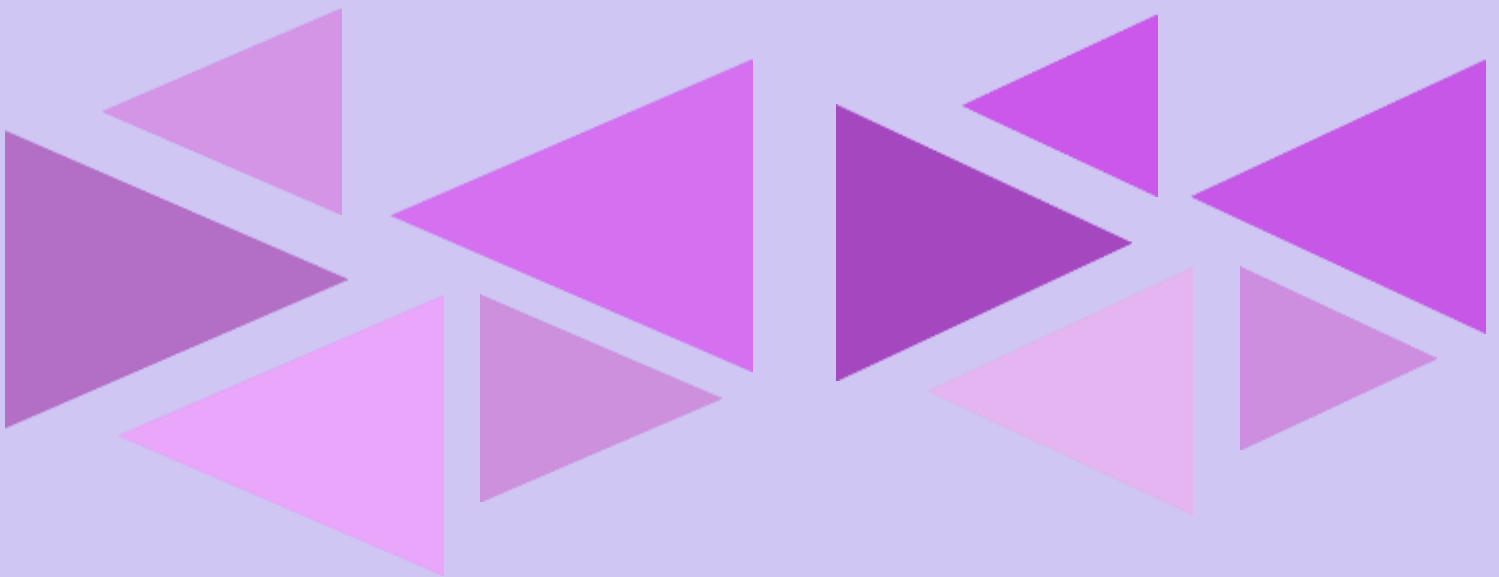




# **HVPS Law Review (HLR)**

Annual Research Journal

**NATIONAL CONFERENCE ON  
EMERGING CRIME & LAW**  
**January 07, 2023**



**Editor in Chief**

**Dr. (Mrs.) Madhura Kalamkar**

**Published by-**

**HINDI VIDYA PRACHAR SAMITI'S COLLEGE OF LAW**

**R. J. College Premises, Ghatkopar, Mumbai-86, Maharashtra**

## **Report of the Conference**

On 7th January, 2023 the Hindi Vidya Prachar Samiti's College of Law organized a One-Day National Conference on the topic 'Emerging Crimes and Law' with the support of the Hon'ble management of Hindi Vidya Prachar Samiti, especially Dr. Rajendra Singh, President and Dr. Usha Mukandan, Director. The Conference was graced by several resource persons and students across the country. Few of such dignitaries were Mr. Rajesh Khushalani, ASI Cyber Crime Department Mumbai Police, Dr. Jitendra Chitnis, Advocate Small Causes Court, Mr. Sumit Rai who also is a legal luminary and has pursued a PG diploma in Cyberlaw, Dr. U.K. Nambiar, Principal MCT College of Law, Mumbai and Dr. Paromita Chatteraj, Associate Professor at KIIT School of Law, Bhubaneswar, The event started with the Lighting of the Lamp & Felicitation of the dignitaries. Thereafter, a welcoming note was delivered by the Hon'ble Principal, Dr. Madhura Kalamkar. She humbly welcomed the resource persons and threw some light on the topic of the day. Thereafter, the resource persons delivered their talk on different forms of Crime and the paradigm change in its concepts at the present time. There were discussions and deliberations on matters like Cyber Threat and Cyber Security, Digital Rape, Crime against Environment and many other. Paper presenters from various Institutes visited and presented their views in the event. The papers presentation session was moderated by Dr. Frances Vaidya, Associate Professor at Gandhi Shikshan Bhavan's Smt Surajba College of Education. Lastly, the programme ended with a vote of thanks delivered by the co-ordinators of the event, Mrs. Rituparna De, and Ms. Shriya Prabhu Assistant Professors, Hindi Vidya Prachar Samiti's College of Law. The event turned out to be a huge success with the guidance of Hon'ble Principal, Dr. Madhura Kalamkar and the IQAC cell coordinator Asst. Prof. Amar Salve.

# **Acknowledgement**

The editor expresses gratitude to all of the contributors for their assistance throughout the entire processing period, including the various faculty members, professionals, and academicians who contributed their expertise, knowledge, and experience.

A special thanks to the management of HVPS, without their support and guidance this national level conference would not be possible. Also thanks to the authors of the research paper who assist in making the conference a grand success.

# **Organizing Committee**

## **PATRONS**

Dr. Rajendra Singh (Hon'ble President, HVPS)  
Dr. Usha Mukundan (Hon'ble Director, HVPS)

## **CONVENER**

Dr. (Mrs.) Madhura Kalamkar (I/C Principal)

## **IQAC Coordinator**

Mr. Amar Salve (Asst. Professor)

## **Editorial Board**

Ms. Rituparna De (Asst. professor)  
Ms. Tanavi Naik (Asst. Professor)  
Mr. Divyang Potdar (Asst. Professor)  
Ms. Neha Naik (Librarian)

## **Advisory Board**

Dr. Swati Routela, Head, Dept Law, UOM  
Dr. Anil Variath, Registrar, MNLU, Mumbai  
Dr. U K Nambiar, Principal, MCT College of Law, Navi Mumbai

**HVPS Law Review**  
**Vol. 01 – Issue -01**  
**Year 2022**  
**E-ISSN: 2584-0746**

Sr. No.	VOLUME- 01 ISSUE 01, 2022 Published by : HVPS College of Law HVPS LAW REVIEW		Page No.
1	Author Paper Title	Ekta Chandrakar <b>POLICE REFORMS: VIA PRAKASH SINGH JUDGEMENT</b>	1-5
2	Author Paper Title	Arkaprava Bhattacharya <b>SEDITION LAW- PAST AND CURRENT TIME</b>	6-11
3	Author Paper Title	Ranjan Kumar Ray and Soumyadeep Chakrabarti <b>THE OUTBREAK OF COVID-19: A REVOLUTION IN THE REGIME OF I.P. AND COMPETITION LAW</b>	12-26
4	Author Paper Title	Shaikh Zeeshan <b>CRIME AGAINST ENVIRONMENT</b>	27-32
5	Author Paper Title	-Manojkumar J. Naik <b>THE LEGISLATIVE FRAMEWORK FOR PREVENTION OF DIGITAL RAPE IN INDIA: A CRITICAL STUDY</b>	33-38
6	Author Paper Title	Samruddhi R. Patil and Aditya Deshmukh <b>BYSEXUALITY IN MODERN SOCIETY</b>	39-46
7	Author Paper Title	Ramashankar Dasharath Singh <b>CYBER TERRIRISM AND LAW</b>	47-67
8	Author Paper Title	Shubhangi Adre <b>DATA PROTECTION AND ANTI- MONEY LAUNDERING – A COMPLEX RELATIONSHIP</b>	68-73
9	Author Paper Title	Joshua Ebenezer <b>SCOMET- EXPORT CONTROL AND WHY S IMPERATIVE FOR INDIA</b>	74-81
10	Author Paper Title	Keval Govardhan Ukey and Amar Suresh Salve <b>LEGALITY OF PROSTITUTION IN INDIA – A JURISPRUDENTIAL ASPECT WITH REGARDS TO SAFEGUARDING AND REHABILITATION OF SEX WORKERS.</b>	82-89

## POLICE REFORMS: VIA PRAAKASH SINGH JUDGEMENT

-Ekta Chandrakar<sup>1</sup>

### Abstract

In India, the necessity for police reform has long been acknowledged. Government-created committees and commissions have been debating the issue for almost 30 years. The National Police Commission (NPC) was also established with the goal of reporting on policing and making reform suggestions. The Commission created a Model Police Act in addition to eight reports and several topic-specific suggestions. However, the majority of the recommendations were not taken up by any administration. Due to this, two former Director Generals of Police (DGPs) petitioned the Supreme Court in 1996, requesting that the court order governments to carry out the NPC recommendations. Following this few more committees were constituted but virtually nothing was ever done to enhance police or put any of these committees or commissions suggestions into practice. Only ten years later, in 2006, the Court issue its ruling in these particular issues. The Supreme Court mandated change in the Prakash Singh case, as it is known in popular culture. Seven binding orders that would help reform get started were given to the states and union territories. These instructions combined the many lines of development produced since 1979. The Court mandated that its instructions be carried out immediately, either by means of executive directives or new police law.

**Keywords:** Police, Legislation, Commission, Investigation, Reforms

### Introduction

The public, now a days, demands for an effective, efficient, accountable, and people-centered police force that consistently tries to uphold the Rule of Law in all the situations they face. Since independence, the National Police Commission, as well as a number of committees, has issued various reports urging comprehensive and detailed police reforms. But, these recommendations have largely gone unheeded and unnoticed.

---

<sup>1</sup> Assistant Professor of Law, Kalinga University, Naya Raipur, Chhattisgarh

Hence, in the year 1996, looking at the urgency of the situation, Prakash Singh, who himself was a police officer and served as DGP of UP Police and Assam Police filed a PIL in the Supreme Court after his retirement. Being, a police officer, he was aware of the ground level situation and therefore he prayed for bringing police reforms. The petition was filed under Article 32 of the constitution praying the Government of India to come up with the new Police Act solely based on the model Act drafted by the National Police Commission and also to implement its recommendations, so as to make sure that the police are completely answerable to the citizens and the legislation of the nation. The petitioner also contended to seek directions to establish various commissions and boards ensuring that the police officers can perform their duties without any fear and to separate investigation wing free from any interferences of executive.

On 25<sup>th</sup> September, 2005, the Government of India again constituted a committee called as the Sorabjee Committee<sup>2</sup> which was entrusted with drafting an outline for a new Police Act. However, the court in this case was of view that no doubt that this committee will come up with report which will prove out be very useful, but the court cannot wait further for the Governments to take appropriate actions to implement changes. Thus looking at the gravity of the problem for preserving Rule of law as there was uncertainty when will the police reforms would be introduced, the court issued appropriate directions for immediate compliance. The suggestions provided will be in effect until the government prepares a new model police act.

### **Analysis and Directives issued by the Apex Court in Prakash Singh & Ors vs. Union of India and Ors<sup>3</sup>**

Article 32 of Constitution of India: Under this Article one can approach Supreme Court for enforcement of their rights. The Supreme Court under this, too have the power to issue directions for the enforcement of any rights.

Article 142 of Constitution of India: The Supreme Court can issue orders to do complete justice on any case before it or pending before it. The directions so issued will be applicable throughout the territory of India.

---

<sup>2</sup> Enactment of New Police Act, Ministry of Home Affairs, PIB Delhi

<sup>3</sup> (2006) 8 SCC 1

Article 144 of Constitution of India: All authorities, civil and judicial residing in the territory of India, shall have to act in accordance of the directions of the Supreme Court.

The effectiveness of any criminal justice system is primarily dependent on the police force's performance. It is one of the most important institutions of criminal justice system which must comply with the rule of law to ensure justice. They are the only ones who come forward at the time of emergency and are the first responders of any criminal activity.

Looking at the urgency of the situation as police were abusing their powers, the court in this case issued certain directives to be complied by both the Central and State Government till proper legislation is framed in this regard and these are:

- A State security commission should be constituted in each and every state. This commission will lay broad policies for functioning of police, will evaluate the performance of police and will ensure that the executives are not exercising any kind of unwarranted influence on the police. This commission will act as a watchdog as also the members of this commission will be someone who does not belong from the Government.
- Police establishment board should be constituted in every state which will be empowered to take decisions related to postings, transfers and promotions for the officers who are below the rank of DSP and will be eligible to make recommendations for higher posts to the appropriate government.
- Police complaints Authorities should be constituted both at district and state level which will make inquiries related to severe charges of police misconduct and misuse of authority.
- To safeguard DGPs and other critical police officers against arbitrary transfers and postings, they should be posted for a two-year minimum term.
- It must be ensured that any state's DGP should be chosen from among the UPSC's top three senior officials, who have been chosen for advancement based on their length of service, good office records, and experience.
- The investigation wing should be separated from the executive wings so as to ensure a faster inquiry, more competence, and enhanced public relations.
- A national security commission should also be established. This commission will help in short listing the candidates for appointment to Chiefs of central police organizations.

Despite of such great efforts made by the Supreme Court which issued directives to be implemented so as to prevent the plaguing of the system of policing in the country, no such positive response has been found by the state governments in this respect. After the directives were issued initially, the Supreme was itself taking care, as in whether directives are being implemented properly or not. It also set up some committees to supervise its progress. Justice Thomas committee is one such



committee which was monitoring its progress submitted its report in the year 2010. After going through the report, the court found that there is total indifference to the issue of reforms.

A review of a study prepared by Niti Aayog in the year 2016 and the “Status of policing in India Report 2019” published by Common Cause, an NGO, and a few other related organisations, shows a dismal image of court orders being followed around the country.<sup>4</sup> There is no evidence to show that something positive has been achieved since then to address the deficiencies identified in the directives given in the case.

In a study released on September 22, 2020, the Commonwealth Human Rights Initiative (CHRI) found that not a single state has completely consistent and complied with the Supreme Court's orders, and that while 18 states enacted or revised their Police Acts during this period, but none of them fully matches the directives stated. The proposed reforms have only been implemented in the North-Eastern nations properly and in practice.<sup>5</sup>

The primary role of the police is to maintain and enforce laws in force, investigate the matter of crimes, ensure security of the people living in the country. But we, however, observe that police being an agency of the criminal justice system is not performing its role properly. They are misusing their powers which are not being monitored resulting in major abuses of people's rights. The infrastructure is also in need of improvement. These issues have their origins in the Police Act, 1861 which is still in effect today. As a result, there is an immediate need to redefine police functions so that they can be held accountable for their blatant act.

It's been 30 years since the National police commission, 15 year since Sorabjee committee had submitted its report and 15 years of Prakash Singh's case. It's high time to implement all the core recommendations issued in these reports and in this case. The government should no longer wait to enact a proper legislation in this behalf and according to the today's need. India now has made rapid advances and our police force cannot afford to be stuck in a bygone age. The internet and digital social media which are rapidly transforming are fueling an explosion of crimes and scope of violence which is leading to unprecedented lawlessness and terrifying aspects of global terrorism.

---

<sup>4</sup> Police Adequacy and working conditions, Status of policing in India Report 2019, Common Cause & Lokniti – Centre for the Study Developing Societies (CSDS)

<sup>5</sup> COMMONWEALTH HUMAN RIGHTS INITIATIVE (CHRI), <https://www.humanrightsinitiative.org/content/police-reforms> (last visited Jan. 9, 2023).

Thus, there is an immediate need to improve our Criminal Justice System and our grassroots level policing institutions. Traditional and sequential devices used in the past to achieve police accountability will not be adequate. It is high time to train our police to deal with current and new challenge and to strengthen its investigation capability free from executive interference. The urgent need is to enact an All-India Police Act wherein all states must be bound to obey it. In this respect, minor exceptions could be provided in special cases relating to the situation in a specific state. Implementing and enacting all the above recommendations could only form part of the solution.

## **Conclusion**

However, it can be said that in effect, the nation has lost its historic chance to modernise and strengthen the police force. But still the time is ripe even now for the states to implement the reforms suggested in the case. The respective government need to understand that police today is not trusted by the citizen of the country. It is believed that they are corrupted, politicized and incompetent. It is said that, reforms starts at home and hence the political leaders should take initiatives from their side and should put pressure upon their respective state governments to implement the directives given in the Prakash Singh's case. The criminal justice system cannot survive without an independent police and investigation department, so having a competent police force is essential.

Transformative changes in the Indian Police are achievable only through appropriate investments in capacity development and attitudinal training aiming for ambitious and substantive reforms. Engagement by all stakeholders is required to accelerate a national movement for transformation, all while bearing in mind the challenging circumstances in which our police system operates. Thus, the vaccine is already there in the form of directives and recommendations, it's just that there is a need for a proper mechanism so that it can be administered to all the states effectively.

## SEDITION LAW- PAST AND CURRENT TIME

*Arkaprava Bhattacharya<sup>6</sup>*

### **Abstract**

Sedition is widely considered as a draconian law from its inception. The urge of the common mass to raise their voice against the political sovereign has been considered as an inherent right in a democratic society. An informed and a participative citizenry whose aim is to refine the law making process via constructive criticisms is a boon for a country. The purpose of a protest should not be violence; it should not alter the integrity of the nation. This basic principle is already there in law which makes it less dark as it is being resembled. Even the common mass can criticize the executive actions too.

Thomas Babington Macaulay in his draft did mention ‘Sedition’ under section 113 but when Indian Penal Code was first passed it wasn’t there. In 1890 through special Act XVII it was added under 124 A. If we compare the then law with the English law, it is a matter of astonishment that the law which was present in England was more deterrent as ‘seditious feelings’ were also taken into consideration. The Act was a catastrophe for Indians; history is the ultimate evidence because from Bal Gangadhar Tilak to Mahatma Gandhi all were victims of this law.

The intention of writing this research paper is to equate the actual pragmatic balance which the present law is providing by analyzing the trail from the colonial regime to modern era. The purpose of a law is to balance the society which will help in maximizing happiness and minimizing friction. In my doctrinal I have pointed out the evolution of sedition law with its current developments. I have also explained why this law is in ‘Abeyance’

**keywords** – Sedition, Abeyance, Indian Penal Code, 1860,

### **1. Introduction**

The shift from restorative form of justice to retributive is the biggest pattern which we have observed in the colonial regime. The abusive laws can’t be ignored as it displayed the real picture and the

---

<sup>6</sup> Student, BBA LLB IX Semester, Indian Institute of Legal Studies, Siliguri.

intentions of the Englishmen. Gandhi once called sedition law "The prince among the political provisions of the Indian Penal Code intended to curtail citizen liberty".<sup>7</sup>

The misuse of the law makes it infamous. Democracy is all about the voice of the people. The common citizen is the heart and soul of the above mentioned form of government and restriction of dissent arbitrarily via any legislative mechanism destroys the whole idea of the formation of this government. The right to raise voice peacefully forms the bedrock of any republic, it is interesting to note that the law at present which is subsisting allows peaceful protests but the fact is that the misinterpretation and misuse of the law is creating all the cacophony.

The blatant criticism of the law isn't an appreciable certitude as the aim of the law had always been to bring balance. The History of this controversial section will help to give a conclusion about the impact of the law in the Indian Society.

## **2. Sedition law and the colonial regime**

### **2.1 Sedition law in England**

The initial purpose of the centuries-old sedition laws was to safeguard the Monarch and the government against any potential insurrection. The statutes forbade any seditious activities, speech, publications, writing, or other expressions. "Encouraging the violent overthrow of democratic institutions" is a general definition of this goal.<sup>8</sup> The following actions are frequently given as examples of those that may be deemed seditious if they are carried out with the intention of inciting violence:

Causing hatred, contempt, or inciting disaffection against the Crown, the government, the constitution, either House of Parliament, or the administration of justice are among those that may be deemed seditious if they are done with the intent to incite violence. In addition, inciting people to try to illegally change matters of the church or state established by law, stirring up crime, or disturbing the peace, is another.

---

<sup>7</sup> Linda Lakhdir, *Sedition law: Why India should break from Britain's abusive legacy* (Feb. 2, 2023), <https://scroll.in/article/1028436/sedition-law-why-india-should-break-from-britains-abusive-legacy>.

<sup>8</sup> (Ex Parte Choudhury, R v. Chief Metropolitan Stipendiary, [1991] 1 QB 429)

## 2.2 Sedition in India

Thomas Babington Macaulay was chosen by the Parliament to lead the First Law Commission, which recommended the development of a penal code during the colonial era. After working on the penal code for two years in 1837, Macaulay completed it. Clause 113(4) of the penal code stated that anyone who makes an effort to stir up feelings of dissatisfaction for the legitimate government of the East India Company's territory among any class of people who live under that government will be punished with expulsion for life or any other term from the territories of the East India Company.

In order to address opposition to colonial rule, the British Government later incorporated this language into Section 124A of the Indian Criminal Code; this particular statute was not included in the I PC's initial design, which was passed in 1860.

The sedition law was mostly utilized in the 19th and 20th centuries to censor speeches and publications by important freedom fighters and Indian nationalists.

The trial of newspaper editor Jogendra Chandra Bose in 1891 is considered to be the earliest instance of sedition ever recorded.

The Bal Gangadhar Tilak and Mahatma Gandhi trials are two of the most well-known instances of sedition law.

### 2.2.1. Bal Gangadhar Tilak Case

The three sedition trials of Bal Gangadhar Tilak, which were widely watched by his followers both domestically and internationally, are one of the most well-known cases. The government alleged that some of his statements about Shivaji killing Afzal Khan were to blame for the next week's killings of the despised Plague Commissioner Rand and Lieutenant Ayherst, a fellow British officer. The two officers were assassinated while they were leaving Government House in Pune after commemorating the Diamond Jubilee of Queen Victoria's reign and going to a dinner function there. Tilak was found guilty of sedition but released in 1898 as a result of the involvement of well-known individuals from throughout the world including Max Weber on the condition that he would not use his acts, speech, or writing to incite unrest.

The case of **Annie Besant v. Advocate General of Madras**<sup>9</sup> is another well-known ruling. The issue concerned Section 124A-like language in Section 4(1) of the Indian Press Act of 1910. The applicable

provision stated that any press used for printing or publishing newspapers, books, or other documents that contained words, signs, or other visible representations that were likely to incite hatred or contempt for the government was prohibited. The Privy Council confiscated the deposit for Annie Besant's printing press in accordance with the earlier interpretation of Justice Strachey.

One of the harshest critics of the law was Jawaharlal Nehru, India's first prime minister following its independence from British. According to a report of the 1951 parliamentary debate on free speech in the Hindu newspaper, he declared that the sedition statute "is exceedingly disagreeable and obnoxious...the sooner we do rid of it, the better."

The idea behind the sedition law is that it prohibits the use of power unfairly. If someone criticizes the policies of the Indian government without intending to incite hatred in others, the law can be heavily utilized by political leaders who find it difficult to accept legitimate criticism from the public. Logically, the requirements listed in Section 124A of the IPC for the Sedition legislation to be charged have very broad parameters, which is why it can be difficult to apply in some circumstances and is quickly abused to punish persons who are innocent.

### **3. Sedition Law Post Independence**

The Constituent Assembly disputed the validity of the sedition statute after India gained its independence in 1947. The Constituent Assembly opted to strike the word "sedition" from the constitution after a contentious discussion (despite keeping Section 124-A of the IPC). But the problematic law was passed by the administration of Jawaharlal Nehru, India's first Prime Minister, in the form of the contentious First Amendment. The Nehru government not only reinstated the sedition law, but also strengthened the colonial law by adding two expressions - "friendly relations with a foreign state" and "public order" - as grounds for imposing "reasonable restrictions" on free speech under Article 19. (2).<sup>10</sup>

Section 124-A, however, became a cognizable offence under a new Code of Criminal Procedure during Indira Gandhi's administration in 1973. This gave police the authority to arrest people without a warrant.

---

<sup>9</sup> Annie Besant v. Advocate General of Madras (1919) 21 BOMLR 867

<sup>10</sup> The Indian Constitution, 1950

### 3. Why the law is a concern?

The colonial law has been a helpful instrument for the police and other state institutions since it was reinstated in 1951 for spreading fear in the population and stifling genuine critiques or opposition against governments. Although legal abuse has occurred under every administration that has come before it, it has intensified recently. A examination of recent cases reveals an increase in legal abuse. According to the portal Article 14, 27 sedition cases were filed in connection with the Pulwama tragedy, 22 cases were filed in connection with the coverage of the Hathras gang-rape incident, and 12 cases were brought against prominent protesters opposing the Citizenship Amendment Act (CAA). Seditious actions can include everything from just carrying signs to chanting dissident phrases and delivering personal messages.

In 2021, six famous journalists, including Rajdeep Sar Desai, Mrinal Pande, and Shashi Tharoor, a member of Parliament, were charged for "posting tweets and purposefully circulating fake news" during farmers' rallies in Delhi. A more bizarre misuse of the provision occurred when three Kashmiri students were charged in Agra for allegedly sharing celebratory messages on social media following Pakistan's T20 victory over India.<sup>11</sup>

The Supreme Court clarified that Section 124-A of the Indian Penal Code, 1860, could not be used to suppress free speech and could only be invoked if it could be proven that the seditious speech in question incited violence or would cause public disorder. Because Kedar Nath criticised the Congress party rather than the Indian state, and the speech in question did not incite violence, it did not amount to sedition.

The Supreme Court also stated that the presence of a pernicious proclivity to incite violence is required before invoking the sedition clause. The Court upheld the former Federal Court's interpretation of Section 124-A of the Indian Penal Code, 1860 in [Niharendu Dutt Majumdar Vs King Emperor],<sup>12</sup> which ruled strongly in favour of legitimate criticism of the government and against arbitrary restrictions on freedom of expression. According to the Federal Court, there must be a public disorder or a reasonable likelihood of public disorder to constitute the offence of sedition.

---

<sup>11</sup> **Niranjan Sahoo**, *The Sedition Law: Time to erase the blot on Indian democracy* (Feb. 2, 2023).

<https://www.orfonline.org/expert-speak/sedition-law/>

<sup>12</sup> (1942) FCR 38

#### **4. Conclusion**

Section 124-A of the Indian Penal Code, 1860 appears to be so broad that any attempt to question the functioning of the Indian Government looks to be pointless. This law is draconian in character due to the broad interpretation of this Section and the punishments. It also violates the right to free expression granted by Article 19(1)(a) of the Indian Constitution, making it unlawful. This also contradicts democratic features. Despite substantial progress over the years, this sedition law threatens India's growth. As a result, India's sedition legislation was recently overturned by the Supreme Court. Furthermore, it should be mentioned that this law violates journalists' rights and livelihood

If the country decides not to repeal the sedition law entirely but only partially, the scope of the Section must be changed in such a way that it cannot be widely interpreted and specifies specific actions that would fall within the ambit of the Section. Individual definitions and the scope of terms and punishments would also greatly reduce the arbitrariness involved in 'sedition' law, so that it does not curtail but only limits freedom of speech and expression.



## THE OUTBREAK OF COVID-19: A REVOLUTION IN THE REGIME OF I.P. AND COMPETITION LAW

-RanjanKumarRay<sup>13</sup>

-SoumyadeepChakrabarti<sup>14</sup>

### Abstract

This study's purpose is to emphasize on how Covid-19 Pandemic affects Competition Law and IPR. As a result of the massive COVID-19 corona virus pandemic, practically all new patent-protected technologies are already in use, from COVID-19 prevention and tracking through vaccinations and medical equipment. Patent rights are morally dubious when they conflict with public health. This paper covers numerous approaches for removing patent thickets. Our results show that patent pledges may help ensure procedural and substantive fairness for the public. The advantages of patent guarantees have led several patent holders to remark on the noble corona virus pandemic publicly.

**Keywords** IP rights, IPR, Patent pooling, Competition law, COVID-19

On March 11 March 11, 2020, the World Health Organization (hereafter referred as WHO) proclaimed COVID-19 a pandemic caused by the Severe Acute Respiratory Syndrome corona virus (hereafter referred as SARS-CoV-2). There has been a resurgence of interest in the long-standing public policy debate over the nexus between Intellectual Property Right (hereafter referred as IPR), innovation, and public health access to new medicines and technology since the outbreak of SARS. COVID-19 isn't the first corona virus or pandemic that has ever existed in human history. A "new corona virus" was created in humans by the SARS corona virus. The outbreak started in late 2002 and swiftly grew to 8096 cases and 774 deaths in 30 countries. Despite the lack of a cure, the pandemic finally ended in 2004, with the last case being documented. This year's pandemic, known as COVID-19, is the first since an influenza pandemic known as swine flu, which infected as many as 1.4 billion people globally in the first year following its breakout between spring 2009 and spring 2010. Between 151,700 and 575,400 people died, therefore.

---

<sup>13</sup> Assistant Professor of Law at Kalinga University, Raipur, Chhatisgarh, Contact: 8101639574, Email-  
ranjan.ray@kalingauniversity.ac.in

<sup>14</sup> Assistant Professor of Law at Kalinga University, Raipur, Chhatisgarh, Contact: 9163429861, Email-  
soumyadeep.chakrabarti@kalingauniversity.ac.in

## **Covid-19 and the pharmaceutical industry**

An innovator or property developer may earn from their creative effort or reputation via intellectual property rights. Other forms of intellectual property protection are available. Inventions that are innovative, non-obvious and industrially applicable are eligible for patent protection. It is necessary to have IPRs to identify correctly, plan, market, produce, and defend creative work. Every industry must have its IPR regulations, management, strategy, and so on, according to its place of competence. There will be a need for increased emphasis and approach in the pharmaceutical industry's IPR strategy soon.

The global pharmaceutical industry is driven by scientific knowledge, not industrial know-how, and the Research and Development (hereafter referred as R&D) operations of a corporation are what determines its success. According to some estimates, this has led to a high level of R&D investment in the pharmaceutical industry, which may be as high as 15% of total sales. One of the most challenging tasks in this business is managing innovative risks while still working to gain a competitive advantage over other companies in the field. Research and development in the pharmaceutical industry are fraught with high failure rates. The effect of new medications that do not satisfy stringent safety requirements is often abandoned after an investment of several years' worth. This will cost you some money. From the moment a chemical is first synthesized until the development of a new medication typically takes eight to ten years. It is becoming increasingly important for pharmaceutical companies to change the focus of their research and development efforts away from creating new technologies for producing existing pharmaceuticals and toward creating innovative pharmacological molecules and chemical entities. In the 1980s, there was a shift in research and development focus away from acute illnesses to long-term chronic ailments. Confirming that one has complied with the standards set forth by many regulatory organizations is essential to penetrating the international market.<sup>15</sup>

More documents must be produced to regulatory authorities in the last decade than combined in the prior ten years. Furthermore, the approval process for new medicines has become substantially more time-consuming. The effort required to bring in a profit is increased to compensate for this shortening of the patent term. Biotechnology-derived drugs, particularly that involving gene usage, may face an even more dire situation. The wealthy nations anticipate pressing for stricter pharmaceutical protections soon enough. It's also feasible that multiple governments will institute price controls as a means to an end. In the pharmaceutical industry, cutting costs means preparing for reduced profits

---

<sup>15</sup> M Angell, The pharmaceutical industry—to whom is it accountable? N Engl J Med.(2000)

and spreading out the time it takes to recoup those losses over a more extended period. The pharmaceutical sector, therefore, obviously faces a complex set of rules and regulations. Solutions that both save money and provide advantages in trade have increased in the previous decade to fifteen. Outsourcing research and development, developing partnerships in R&D, and forming strategic alliances are just a few examples.<sup>16</sup>

### **Nature and scope of the pharmaceutical industry**

In the race to discover the secrets of the human genome, new scientific knowledge and technological innovations have emerged that are reshaping the pharmaceutical industry's business model. An advantage for biopharmaceuticals will be that each person's DNA will be mapped and recorded on an implantable chip, allowing for more customized treatment. Using the data on the chips, doctors can prescribe the proper medication. A primary I.P. concern would be storing individuals' personal information in such databases. Biotechnologically created medicines will become more widely available. A biotechnologically-created drug will have a different mechanism of protection than a drug that is not biotechnologically created. The patent document must write down microbiological strains before a drug or vaccine can be made. If the pressure has been found before and written about in scientific papers, it is easy to figure out what it is. Under the Budapest Treaty, strains are discovered, developed, and deposited with international depository authority. These depositories' databases should also be examined as part of a novelty search. Companies rarely share their work, but it is prudent to wait until a patent application has been filed before exposing an invention in journals or seminars.

A registration number must be cited in the patent specification when dealing with microbiological advances, which necessitates depositing the strain at one of the approved depositories. This removes the necessity for writing down a description of anything alive. Depositing a strain, for example, costs money, although not much if one is not working with cell lines. Furthermore, as in the past, sequences including genes, gene expression, DNA, and RNA must be described in the patent specification. Companies create alliances for several reasons, such as pooling R&D resources and facilities, gaining access to distribution channels, or sharing production resources. Any time you enter an R&D alliance, it's best to formalize your agreements to address issues like I.P. ownership in several countries, cost-sharing to obtain and maintain I.P. and revenue generated by that I.P. trade secret protection, and dispute resolution. It's important to remember that an alliance will be more successful if one of the parties has a more robust I.P. portfolio. This agreement may have additional terms.

---

<sup>16</sup> Mrudula BS, Durgadevi NK, Mahadevi BR, Tejeswi B, Durga P.V., Intellectual Property Rights Pinpoint at IPR Spotlights converted R and D, Drug Inv Today, v 2 197-201 (2009)

Soon, many pharmaceutical companies will contract research with universities, commercial R&D organizations, and government R&D facilities in India and worldwide. Everything described above will be helpful. Keeping studies under wraps will need additional attention.

Intellectual property rights are being overused and abused in the pharmaceutical industry at the expense of consumer welfare and competitiveness. This shows the injustice at the cost of the public benefit when the pharmaceutical sector refuses to take any risks and innovates. Legal reform alone is not enough to correct this injustice. Antitrust law must intervene effectively, even if Congress tries to close loopholes in existing rules and introduce new legislation to limit even more unfair economic practices by the pharmaceutical industry. Antitrust laws have rightly scrutinized mergers and acquisitions and non-competition agreements, but other methods must be addressed. Advocacy and brand name development, as well as granting patents on minor aspects of existing medicines, may help antitrust legislation maintain a healthy balance between rewarding innovation and protecting competition. – Antitrust legislation

Natural botanical-based traditional medicine is integral to human health care in many developing and developed countries, increasing its economic value. The study says more than 60 billion dollars have been made in sales, with yearly growth rates ranging from 5 to 15%<sup>17</sup>. Conventional knowledge-based medicines are often claimed to qualify for patent protection. Researchers or businesses may be able to claim IPR on biological resources and traditional knowledge after a minor change. According to patent filings related to herbal medicine<sup>18</sup> this trend is evident. In the case of patent applications for natural goods, traditional herbal medicine, and herbal medicinal items, each country's IPR legislation, which is classified into food, pharmaceuticals, and cosmetic categories as appropriate, is followed. The worldwide organized herbal medicine and cosmetic businesses place a high value on medicinal plants and related plant goods; therefore, they make excellent candidates for patent claims.

## **Patentable Drugs**

Writing a patent specification involves combining scientific, technical, and legal skills that take years to perfect. The claims set out in a patent specification form the nucleus of the patent for which a party seeks to assert ownership. No patent may be issued for discovering a unique property in an already-existing chemical compound. An invention may be patented if it can be used in the real world. It is

---

<sup>17</sup> Abayomi Sofowor, Eyitope Ogunbodede & Adedeji Onayade, *The Role and Place of Medicinal Plants in Strategies for Disease Prevention*, 10(5) AJTCAM (2013)

<sup>18</sup> Ibid

not patentable to find that an already known substance can withstand mechanical stress, but a railway sleeper constructed from the material may be. Scientists have found a brand-new characteristic even if a sense isn't brand new. If the combination of well-known substances generates a unique effect, it may be possible to patent it. Insecticides, fertilizers, and medications have never previously been made using this combination. A scientist may have discovered a new molecule, but its structure remains a mystery. The description of the material, its properties, and the process by which it was made will be critical in this case.

Combining well-known substances into valuable products may be patentable if the elements have a functional link when combined. No chemical reaction takes place in this situation at all. A very minimal amount of protection is provided by it. The patent does not cover individual components of the combination. For example, a patent on aqua regia does not preclude someone from mixing the two acids in varying amounts and asking for further patents. “As a result, most countries—except for the United States—do not allow the patenting of human or animal medicinal procedures. Precaution should be exercised while making claims about the unique therapeutic application of a well-known substance. Medications, including herbal ones, account for the vast bulk of the submissions. Among the few applications are engineering, electronics, and chemicals. Approximately 62% of all applications are for drugs and treatments. Patent holders may be able to contribute to the allocation of scarce medical resources by commercializing health-related intellectual technologies. The WHO has licensed multiple COVID-19 vaccinations, and many repurposing drugs have been developed for COVID-19. For developing countries and the poor, patent guarantees from companies like AbbVie and Moderna, Inc. may make it easier for generic drug manufacturers to get free patent licensing, increasing access to medications and vaccinations.

### **Significance of the Patent Cooperation Treaty**

The Patent Cooperation Treaty (hereafter referred as PCT), founded in 1978, is an example of a multilateral agreement to safeguard intellectual property rights. By indicating which countries they are interested in within their PCT application, an inventor from a country that is a contracting state in the PCT can simultaneously gain priority for their innovation within all of the member countries or just one of them. All PCT-related endeavors are coordinated by the World Intellectual Property Organization (hereafter referred as WIPO), which calls Geneva, Switzerland, home. It is necessary to submit a unique patent application for protection in each country of interest. In some instances, this must be done within a predetermined time to maintain priority in these countries. A significant

amount of money would need to be invested in a relatively short time to cover expenses like those associated with filing, translation, and legal representation. Because there is so little time to decide whether or not to apply for a patent in a particular nation, it is also possible that the assumption may not be fully justified. This could be because the decision-making process takes place in that nation.

Inventors from states that are parties to the PCT can get priority for their ideas without having to file separate applications in the countries that interest them. This helps them save money on costs related to translation and other expenses. Under the terms of the new agreement, it provides member countries with significantly more lead time to submit patent applications. Following the Paris Convention, priority in other countries can be obtained after an initial filing has been made for 12 months. The period of protection under the PCT can be between 20 and 31 months. Inventors can benefit from a search report as part of the PCT process to ensure that the claimed invention is novel. Before filing for protection in other countries, the inventor may wish to increase their certainty about the invention's patentability by requesting a preliminary evaluation to increase the likelihood that the invention will be granted a patent.

### **Patent pledge: an implications in the context of Covid-19**

Making commitments regarding patents is relatively new and is not permitted by either domestic law or international conventions. To foster technological innovation, most nations' legal systems now include provisions for patenting new inventions and ensuring their protection. The majority of businesses, in the majority of instances, actively pursue high-cost patent licencing alternatives in addition to rigorously enforcing their patent rights. On the other hand, patent pledgors are individuals who have taken the initiative to give up some of their patent rights in exchange for greater access to technology markets. In this case, the patent rights are traded for greater market access. For instance, the Open COVID Pledge and the Open COVID-19 Declaration do not enforce patent rights against anyone who uses the promised patents to defend COVID-19. From a sociological point of view, patent obligations might be able to contribute to an overall improvement in the health and happiness of society. An incentive in the form of a patent pledge is offered to patent holders in the hope that they will agree to move away from the conventional licencing model and toward the open approach. Most parties involved in patent litigation do not attempt to have long-term patent infringements halted by either a temporary or permanent injunction. Some patent holders have committed that they will not go after patent royalties for a set period. This is only a possibility if the other party satisfies a set of conditions that have been established.

People who take the Open COVID Pledge or participate in Open COVID-19 agree not to seek monetary compensation or use patent rights. Intellectual property owners make significant economic decisions when they give up certain rights. This decision may benefit society as a whole and does not harm any organizations or individuals. The holders of patents will experience short-term losses as a direct consequence of the guarantee of patent rights. In the long run, a patent holder may acquire competitive advantages and opportunities for partnership if they implement a long-term development strategy or make an effort to improve public health.<sup>19</sup>

Patent pledges cannot safeguard all members' common interests because of their many complex patent promises. It's not uncommon to see a patent promise with conditions attached, such as a restriction on the technology, a location, or expiration date. As a result, the vast majority of patent promises will be able to be used under the connected requirement rather than under all circumstances. Making a patent promise as part of an open patent strategy can help companies address the conflict between exclusive patent rights and the interests of society as a whole. Following an available patent strategy, companies may promise to distribute their patent licences. Procedural fairness considerations favour patentees, not third parties, in the patent commitment process.

Since Open COVID Pledge has made the standard requirements available on its official website, it may encourage more small and medium-sized businesses to sign patent pledges opposing Open COVID-19. As soon as they've submitted commitments, patent holders are expected to keep their promises not to sue or seek compensation for anything, including using their patent rights to stop the spread of COVID-19. As a result of patent promises, a community's common good and social well-being are protected since patent holders give up part of their related patent rights.

### **Importance of a patent pledge**

Several methods may be used to clear patent thickets. Efficiency studies show that patent holders that join to assert their rights during the COVID-19 outbreak will do better than their pledgors who opt out. To resist COVID-19, many patent holders made pledges rather than instituting compulsory licensing or joining patent pools. As part of our investigation of the advantages of patent promises, we evaluate three methods for avoiding patent disputes from an ethical perspective.

---

<sup>19</sup> Xiaodong Yuan & Xiaotao, "Pleading Patent Right For Fighting Against the COVID-19: From the Ethical and Efficiency Perspective" *J Bus Ethics* (June 17 June 17, 2021) available @ <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8211307/>

TRIPS establish minimum requirements for the protection of intellectual property for the 164 members of the World Trade Organization (WTO). Member states' licensing policies should adhere to Article 31<sup>20</sup>, although they differ from one another. Thus, Article 31<sup>21</sup> is used as a case study to analyze compelled licensing from both an efficiency and corporate ethical perspective. Patent promises are beneficial in the fight against the COVID-19 epidemic.

Making a patent promise is simpler and more manageable from a procedural fairness aspect than creating a patent pool or issuing a compelled license. To understand compulsory licensing, one must consider it a specific claim that a government must grant. In contrast, patent pooling may be seen as a collective activity in which numerous patent owners are willing to enter into licence agreements. Compulsory licensing or organizing a patent pool is a long and tedious procedure. On the other hand, patent promises are specific pledges or commitments to provide patent licenses. Due to standardized patent pledges like Open COVID Pledge-Patent, patent holders have an easier time fulfilling their agreements to provide patent rights. A growing number of small and medium-sized enterprises are making patent commitments to fight COVID-19 because of the simplicity of the process.

Second, patent pledges will allow patent holders to give up some of their rights, which will help the general public achieve the highest possible level of substantive justice. Two types of patent promises can be made regarding COVID-19: unilateral and coordinated. Unilateral patent promises with specific conditions offer various options, including free licenses or non-discriminatory royalty rates. There must be no injunction against patented technology users, regardless of the kind of patent promise made by the patent owners. The ability of patent holders to get international licensing may be enhanced by the fact that patent obligations may cross national borders. Due to patent commitments, generic drug makers are compelled to manufacture COVID-19 drugs or vaccines under an open license. Increasing the availability of medicines and vaccines in the case of the COVID-19 pandemic will significantly boost access to life-saving therapies. As patent holders give up more rights, the public gains more from their obligations.

It can decrease the conflict between public health and intellectual rights by balancing patent promises' short-term costs and benefits. The COVID-19 pandemic necessitated the voluntary surrender of patent holders of some rights. For a specific time, patent holders give up their secured patent rights. However, patent rights will be restored after the COVID-19 outbreak is over. In the long run, patent holders will develop a reputation for social responsibility and have more possibilities for licencing their patent despite the short-term loss of money.<sup>22</sup>

---

<sup>20</sup> Supra note 107

<sup>21</sup> Ibid

<sup>22</sup> Supra note 127



## **Advantages of patent pledge**

A long-term strategy of free patent licencing will harm businesses' long-term growth. Protecting patent rights is essential for the medical industry to innovate and flourish. Making new medicines and vaccines costs a lot of time, money, and effort, but there are also a lot of risks involved. Patent protection may help the pharmaceutical industry's bottom line by preventing innovations from being copied.

A fair global distribution of medical resources for COVID-19 can't be achieved just by relying on patent obligations. Because of patent promises, the supply of medications and vaccines will not be significantly enhanced if no generic manufacturers create pharmaceuticals or vaccinations for COVID-19. Since they connect research and development to products, patents are frequently seen as significant outputs of innovation activities and crucial technological resources for new product creation.<sup>23</sup>.

## **Disadvantages of patent pledges**

Patent promises may be unsustainable for an extended period if no accompanying supportive measures exist. As a consequence of our findings, policymakers and business leaders will be better equipped to address public health crises using patent portfolios.

The Open COVID Pledge and Open COVID-19 have been formed to counteract COVID-19, which has increased in firms signing patent agreements. The paper examines the advantages and cons of patent agreements using an analytical methodology that incorporates efficiency and corporate ethics. The management must deal with the ramifications of our findings.

Patent holders should be encouraged to make active pledges in their fight against COVID-19, either by the WHO or the WIPO. For access to patented health innovations, patent holders agree to give up some of their rights, such as the right to seek injunctive relief against patent users. As of April 2021, SAGE recommends several vaccines for COVID-19, with 88 currently in clinical trials and 184 in the pre-clinical stages. Patent pledges for COVID-19 have been made by just a few companies, including Moderna, which has a patent for its mRNA-1273 vaccine. More pharmaceutical and vaccine patent holders should sign on to the WHO's suggested patent pools, C-TAC or MPP so that the pools may be formed as quickly as possible.

National governments should be more involved in developing and distributing COVID-19 treatments and vaccines—unaffordable assurances of free patent protection for companies who have invested

---

<sup>23</sup> Ibid

Significantly in developing new medical technologies. The government of a country is obligated by law to provide for the people's medical needs. To address the disadvantages of patent promises, national governments should give various legislative mechanisms to boost COVID-19 health technology. There are several ways in which public monies may be used to support the development of health technology, such as by providing funding to national firms or by purchasing healthcare services for the general population. Consequently, patent holders can meet their promises in the face of government support.

Third, in the wake of the global COVID-19 outbreak, corporations should consider making a patent guarantee, whether unilaterally or in concert with other companies. There can be little doubt that patent entanglement will hinder the use of valuable medications to improve public health. To get through the patent maze created by the COVID-19 epidemic using traditional methods such as voluntary licensing or patent pools is nearly impossible. COVID-19 manufacturers can use proprietary health technologies because of patent agreements. Life-saving healthcare may become more accessible as diagnostics, treatments, and vaccines become more widely available. The COVID-19 pandemic will be contained and finally extinguished if international organizations and national governments, patent holders, and manufacturers work together.

Managing I.P. and IPR is a complicated process that includes several activities and procedures that must comply with national and international treaties and conventions. It's no longer solely a matter of national interest anymore. I.P. and its associated rights are heavily influenced by various factors, including consumer demand, market response, and the financial burden of commercializing an invention. So, in other words, trade and commerce are critical in the administration of IPRs. Many kinds of IPR need various approaches to managing, planning for, and preparing for, as well as the engagement of personnel with a wide range of subject-matter expertise. There should be different I.P. regulations, management styles, and strategies for each industry based on its area of competence. The pharmaceutical industry is implementing a new I.P. strategy. Because of the increasing chance that particular IPRs are invalid, antitrust law must intervene to ensure that illegitimate, though limited, monopolies in the pharmaceutical industry are not built and maintained unlawfully. There is still a slew of concerns to be resolved in this context.<sup>24</sup>

### **4.3. Waiver of I.P.: amidst Covid-19**

With the wealthiest countries currently holding a large portion of the global supply of covid-19 vaccines, intellectual property rights must be waived to alleviate this inequality. As of April 30 April

---

<sup>24</sup> Ibid

30, 1.3 billion doses have been delivered worldwide, but just 0.2 per cent of those doses to low-income countries. I.P. waivers have the unfortunate effect of allowing competitors to get expensive innovations more quickly. Because vaccine components are rare and it may take years to build up manufacturing capacity from the ground up, companies argue that I.P. relief would not speed up vaccine production.

Other nations argue that governments can already seek 'compulsory licensing' to bypass intellectual property laws in times of crisis. The World Trade Organization is now reviewing Bolivia's request to import COVID vaccines in this method. Additionally, the European Union claims that the United States is obstructing the shipping of COVID-19 vaccinations and the components that go with them. Bringing this up is appropriate. Pandemic restrictions would need to be eased in the case of an outbreak.

They think these are critical problems that need to be dealt with. There are not, however, sufficient reasons to deny I.P. relief. Even as the pandemic worsens, the case for waiving the ban becomes stronger.

Because vaccine manufacturing, research and development are concentrated in a small number of high- and middle-income countries, there is a severe problem. The great majority of vaccine doses have been sold to governments in high-income nations by companies based in these countries, who also hold the majority of the intellectual property. Out of the 8.6 billion confirmed orders, 6 billion doses have been pre-ordered by governments in high- and middle-income countries.

European nations committed at the Global Health Summit in Rome last week, just before the World Health Assembly in Geneva, Switzerland, to share extra vaccine doses with low- and middle-income countries. European Commission President Ursula von der Leyen has also advocated 'clarifying and simplifying the present means for imposing mandatory licensing. ' There is a fair chance that more vaccine funding will be offered during the G7 meeting in the United Kingdom next month.

Pledges like this are vital if we want to stop the spread of the disease. They do not, however, address the fundamental issue - the countries who support the I.P. waiver are not seeking charity but rather the ability to study and produce their vaccines without fear of being sued by patent holders. COVID's I.P. waiver supporters are aware of this basic notion. Those countries' leaders who are still opposed to allowing patents to be waived need to realize this as well. Pharma companies and most nations with high affluence were opposed to the concept at the time. As an alternative, these nations have agreed to boost funding for programmes like COVAX, which provides vaccines to low-income countries. Last month, the United States only recently backed a vaccine I.P. waiver, which was an unexpected and much-needed step forward.

Considering the size of the U.S. pharmaceutical business alone, this choice is of critical significance. I.P. norms have been established and enforced by the United States and other research-intensive nations for decades, most recently via the WTO, where a proposed I.P. waiver is now under discussion. Even a few months ago, the idea that the United States would take such a position was unthinkable. After Japan, South Korea, the United Kingdom, and the European Union have done so, the rest of the world must follow suit.<sup>25</sup>

### **Global approach for the waiver of I.P.**

Covid-19 containment and treatment under the TRIPS Agreement were suggested to the World Trade Organization on October 2, 2020, by both India and South Africa. This initiative aims to reduce obstacles to timely access to inexpensive, appropriate medical items and encourage global immunizations. For the worldwide reaction to be effective, these products must be quickly accessible, and the whole world must cooperate in this effort. According to the Max Planck Institute for Innovation and Competition's recently issued position statement, such a waiver is unlikely to be needed or suitable to achieve the stated goals. The following are some of the study's most significant findings.<sup>26</sup>:-

- A scarcity of raw ingredients, limited production capacity, and, in the case of vector and mRNA vaccines, very sophisticated manufacturing procedures is the principal causes of vaccine delays. A surrender of intellectual property rights cannot solve these difficulties.
- It takes a long time to create a new vaccine because of the many steps involved, starting with the provision of a technological basis and continuing through safety studies and eventual commercialization. However, despite the usual fierce competition in the biopharmaceutical industry, vaccines against Covid-19 are being developed, manufactured, and marketed in unprecedented cooperation.
- Patents are often utilized as a basis for this kind of partnership since they guarantee the performance of obligations. Even a fair abridgement of these rights may have a chilling effect on a party's motivation to work together.

The applicable drug authorities need marketing authorization to put a medical product on the market. Even bio-similars, copies of small-molecule drugs but subject to far tighter regulations than generics,

---

<sup>25</sup> Editorial, "A patent Waiver on COVID vaccines is right and fair", *Nature*, 593, 478(2021) <https://doi.org/10.1038/d41586-021-01242-1>.

<sup>26</sup> Waiver of Intellectual Property Rights", OBLB, (June 29 June 29, 2021) <https://www.law.ox.ac.uk/business-law-blog/blog/2021/06/10-arguments-against-waiver-intellectual-property-rights>

fall under this category. The third party does not need marketing permission if the original manufacturer successfully transferred the licence. Even if all applicable intellectual property rights, including the exclusivity of test results, were waived, each new producer would still be required to get its marketing licence and fulfil safety, quality, and efficacy criteria. If the original manufacturers refuse to cooperate, the transfer of intellectual property rights will inevitably cause a delay.

However, there are several reasons why biosimilars costs would not be considerably lower than those of current goods, such as the following:

- Production facilities, especially new vaccines, need large expenditures, which are unlikely to be lower for bio-similar and show in their price.
- Because the manufacturing and distribution expenditures may be as much as half of the vaccine's price, bio-similar vaccines are unlikely to cut the vaccine's cost significantly.
- Because of the increased competition, vaccination prices and profit margins will become more constrained.
- Vaccines are already available at a reasonable cost from certain vaccine producers and manufacturers.

Article 31 of the Agreement<sup>27</sup> authorizes WTO members to grant patents compulsory licences under specific situations. If patentees refuse to provide production licences for unjustified reasons, member states can incorporate this option into their national law. International law's ability to adapt to the present-day unprecedented conditions is not hampered by the measures taken by particular states, as shown by the information available.

As Covid-19 viruses evolve, we may need new vaccinations to protect against them. Because of this, it is uncertain whether vaccine developers would be willing to invest in new vaccines without patent protection. Patents in other medical fields, such as cancer therapy, also cover Covid-19 vaccines already licensed. To produce the vaccine, fundamental patents would have to be relinquished. Aside from immunizations, this might have unforeseen repercussions in terms of financial incentives for future research and development.

Companies must be able to make a decent return from their R&D investments to motivate them to engage in R&D. The fundamental question is how much justification there is for a specific expenditure. A patent right may not necessarily result in high prices for Covid-19 vaccines, primarily when multiple vaccines compete. Governments supporting vaccine manufacturing should have handled pricing difficulties via equivalent agreements and created legally enforceable standards.

---

<sup>27</sup> Natco V Bayer Compulsory License Application No. 1 of 2011(May 9, 2012)

There must be transparency on the overall investment and the calculation associated with the sale of the resulting medicines and vaccines if taxpayer money is being utilized for pharmaceutical research and development or manufacturing facilities. It is the role of the funding agency to make sure that recipients of its money reveal their costs and pricing structures since private enterprises cannot be expected to do so.

However, any intellectual property rights based on Covid-19 would be relinquished as a part of the proposed TRIPS Agreement renunciation. However, the phrase 'concerning might be interpreted in various ways. Because of the idea that governmental action must be necessary and acceptable, this is problematic. As a result, the extent to which we may waive intellectual property rights for things just accidentally linked to immunizations would be significantly altered.

Promoting equitable access to vaccinations and medications associated with Covid-19 is an issue of international solidarity. The international community must find alternative methods since waiver of intellectual property rights cannot be used to attain this goal. Good governance requires an adequate international legal framework to deal with such global issues in the future. More than 25 countries and organizations, including Germany, have requested a worldwide pandemic treaty. ACT-A and COVAX programmes and other international strategies are being used to control the outbreak in certain areas. Every state that can contribute has to do so. National interests alone and pushing for intellectual property rights waivers will not increase immunization availability in developing countries in the foreseeable future.

## **Conclusion and Recommendation**

Patent protection is advantageous to pharmaceutical companies. When the patent on the original product expires, generic versions of the same product will be available on the market. Competition rules in the European Union may prohibit pharmaceutical companies from attempting to prolong a product's patent protection. As generic items foster the invention of new products, such conduct may have the unintended effect of eliminating incentives to innovate. Furthermore, Astra-Zeneca was discovered to be abusing the patent system, and medical approval process, so generic and parallel imported drugs could not compete with its blockbuster drug. A 60 million euro fine was levied on Astra-Zeneca. Currently, the appeal is being heard by the Court of First Instance. As a result of this first incident, the Commission has intensified its monitoring of competition in the generic pharmaceutical market. Competitor in the human pharmaceutical industry seems to be lacking in Europe, with fewer new medications entering the market and the introduction of generic drugs being delayed from time to time, according to early results. Consequently, the Commission has begun an

inquiry into why this happened.

There is no plan in place in India to allow the I.P. and competition laws to function in harmony at this time. The Indian government and the competition commission of India (hereafter referred as CCI) are unsure how to handle the thorny issue of competition law that intersects with the rights to intellectual property. By allowing Patent Holders to operate freely and within the bounds of competition law without CCI intervention, essential practice theory would enable Patent Holders to thwart patent pooling, which has a detrimental effect on competition and innovation. The I.P. and competition regimes share the primary purpose of benefiting the economy, which is vital to ensure this convergence.

A detailed examination of the Competition Act suggests that the Competition Commission is competent to consult with other sectoral regulators. Still, because the rules are neither mandatory nor binding, this is only partially addressed and executed. The TRIPS also urges countries to improve their I.P. protection systems. As a result, international engagements, as well as international legislation, must be considered. The E.U. and the U.S. have taken a balanced approach in this regard. They believe the abuse of a monopoly market structure by the owner of an intellectual property right to be the exception rather than the rule. Because Indian belief draws mainly on common law, especially in economic direction, both the E.U. and U.S. methods can help policymakers reach a reasoned conclusion or build a flexible policy where I.P. rights and competition law intersect.

The CCI has classified Patent Pooling agreements as restrictive trade practices since they impede India's competitive regime. However, Section 102 of the Indian Patent Act allows for establishing patent pooling agreements that can be administered, maintained, and monitored by the government. The primary concern is whether India's competition law can regulate such deals amidst Covid-19 chaos.

The Indian government requests an intellectual property rights waiver under the Agreement on Trade-Associated Aspects of Intellectual Property Rights. The assumption behind seeking an IPR waiver is that it will allow more companies to manufacture vaccines and medications, increasing their availability at a lower cost. IPR exemptions for COVID-19 vaccines and pharmaceuticals, on the other hand, are unlikely to make a difference. A more successful strategy is using compulsory licences and lowering tariffs and non-tariff measures.

## CRIME AGAINST ENVIRONMENT

*SHAIKH ZEESHAN*

### **ABSTRACT**

Crime against environment is crime against humanity because environmental crimes by humans adversely affects natural environment directly. Humans are also part of natural environment so indirectly all the human race will suffer the adverse effects of those crime which is committed by humans against environment. Concern for environmental protection and preservation started globally in the second half of 20<sup>th</sup> century. Environmental crimes includes all the illegal activities which negatively impact on natural resources, wildlife, ecosystem, biodiversity and natural environment of earth as a whole. If we think deeply about the issue we will find that human greed and ignorance are the main cause of this. Greedy desires to possess more and more wealth and comfort and luxuries have made humans blind because of which humans are not able to see the disastrous effects of their so called material development for which they are ready to degrade, damage and destroy natural environment through their illegal and immoral activities against environment. Because of ignorance humans are not able to realize their interconnectedness with natural environment. By damaging and destroying environment for our selfish purposes, we are unknowingly damaging and destroying ourselves as well as our future generations indirectly. Despite being various laws and regulations related to environment conservation and protection crimes against environment are increasing year by year. Criminals of these crimes deserves reformation and liable for prosecution, fines and imprisonment. Crime against environment includes various activities such as pollution crime, wildlife crime, illegal mining, illegal fishing, illegal logging etc. It is a multi-billion dollar crime industry. They are now known as Ecomafia. This word Ecomafia implies all criminal activities which causes damage to the natural environment. All the leaders of the globe since the last fifty years came to realize the importance of natural environment for human survival therefore this global environmental issue of crime against environment came into forefront. Environment can regenerate itself after few centuries but we can not. Our whole existence is depend of natural environment be it water, air, food, temperature, or other natural resources. We need environment but not vice versa.

**keywords:** Ecomafia, greed, ignorance, interconnectedness, future generations, human survival, conservation, protection, degradation, destruction.



## Introduction

Man is surrounded by biotic and abiotic components together known as environment. Human beings need environment. Environment does not need us. They are not dependent on us for their existence. But our existence is totally dependent on our environment. We can only pollute, degrade and damage environment but we can not keep our environment in the same degraded manner in future time because earth has the limited and slow capacity to regenerate itself. Environmental crime means violation of those laws that are made to protect and preserve environment. It could be irresponsibility, mistake and careless attitude of concerned environment authority and it majorly includes actual illegal dumping of pollutants into environment or extracting natural resources illegally by damaging the natural environment. The degrading quality of environment has threatened the possibility of survival of humans and animals in future on this planet because of various crimes related to environment. Man made activities like industrialization, transportation, technological advancement, agriculture, mining etc. have disturbed the natural balance of our environment.

Environment plays very important role in developing economies, livelihood and livestock. Clean environment provide the platform upon which future food production and life of future generations will depend. There are two types of activities which affects environment weather, and climate. They are natural activities and man made activities. Man made activities are also known as anthropogenic activities. We should plan a comprehensive programme for the prevention and control of air pollution through automobiles. We should lay down new standards for emission of air pollutants into the atmosphere from automobiles.

Desire to have a better living standards in terms of material comforts leads to various types of problems like rise in temperature, low agricultural productivity, loss of ecosystem & biodiversity, deforestation, rise in sea level uncontrolled exploitation of natural resources and various adverse effects on human health. Economic development is need of the hour because human beings wants better standard of living. Better materialistic life style resulted in multiplication of needs and wants and these have accelerated the pace of development to the extent of depletion of natural resources. In the name of development humans have damage the life supporting system of human biology and nature's ecology. The limited natural resources and unlimited human wants have disturb the natural balance between the environment and development. Development should not affects the needs of future generations and such development is known as sustainable development. We must fulfill the needs of the present generation without compromising the needs of the future generations. We have some obligations towards our future generations therefore we should not pollute and degrade our

natural environment so that future generations can also enjoy their life happily in the same manner we are enjoying and using different natural resources like clean air, pure water, fertile soil, favorable climate, healthy food etc.

Environmental problems since last four decades have become a matter of not only national concern but of international importance. Conservation and protection of environment is essential for survival of human beings on this planet. Environment means conditions that surround someone or something. It also means the conditions and influences that affect the growth, health, progress, etc., of someone or something. Now it has been said that human beings are natural environments' worst enemy. The environment proves that all human activities are interconnected with the nature. Law is regarded as a means of controlling human conduct.

Now environmental pollution is a global concern. Pollution means presence of some undesirable substances in air, water, and soil. In Millennium Development Goals environmental sustainability was one of the goal out of eight goals. In Sustainable Development Goals main emphasis was given to environmental related issues like to take urgent action to combat climate change and its impacts, conserve and sustainably use of the oceans, seas and marine resources for sustainable development, protect, restore and promote sustainable use of terrestrial ecosystems.

Stockholm Declaration of 1972 was perhaps the first major attempt to conserve and protect the human environment at the international level. As a consequence of this declaration Indian Parliament inserted two articles i.e., 48A and 51A accordingly in the Constitution. In Indian constitution there are two important articles related to environment conservation and protection. Firstly, Part IV of Indian Constitution that is directive principles of state policy DPSP and its Article 48-A goes like this that The State shall endeavor to protect and improve the environment and to safeguard the forests and wildlife of the country. Secondly, Part IV-A that is Fundamental Duties FDs and Indian citizens' seventh duty (g) goes like this that It is a duty of all citizens to protect and improve the natural environment including forests, lakes, rivers and wild life, and to have compassion for living creatures.

## **Problems and Solutions**

Environmental crimes means violation and deliberate breach of any national or international environmental laws or rules that was created to ensure conservation, protection and sustainability of natural environment. Environmental crimes include illegal trade of wildlife, improper waste disposal, forestry crime, destruction of wetlands, burning garbage, illegal fisheries, illegal logging and trade,

improper handling of insecticide, pesticide and other toxic and hazardous chemicals, falsifying lab data related to environmental regulation, illegal extraction and trade of natural minerals, bribing government officials, wildlife trafficking, smuggling of ozone depleting substances, committing fraud related to environmental crimes. Environmental law in the implementation of environmentally sound development serves to prevent the occurrence of pollution and or destruction of the environment so that the environment and natural resources are not disturbed continuity and carrying capacity. Strict and effective environmental laws will be conducive for the continuation of environmentally friendly development or sustainable development.

These environmental crimes are committed not by chance or accidentally or mistakenly but they are planned and organized crime and the motive behind these types of crimes is to gain material or financial benefits. Violators of environmental law are face penalty fines or punishment of jail time or both. Government has taken so many steps to increase the cases related to environment. Due to awareness, there has been a rise in the activist movement related to environment. Activist movements are the voice of voiceless which is our nature or environment. For tackling the problem of increasing environmental crimes only objective assessment of crime situation is not sufficient because we also need consistent, logical, and non-controversial criminal legislation. Institutional and regulatory failures, poverty, demand, low risks and high profits are some of the main drives behind the environmental crime. Till now huge damaged has been caused to environment by humans for their selfish material wants and this damage is beyond repair but still this harm can be reduced and some recovery of natural environment is possible if people will understand that their and coming generation's life is directly dependent on environment.

Illegal trade in forest and wildlife products, as well as the illegal exploitation of natural resources is now widely recognized as a significant threat to both the environment and sustainable development. The ultimate aim and goal of all the legislations and acts related to environment is to preserve planet, protect environment and prevent pollution of various kinds. Despite of various acts still people are committing crime against environment which indicates that either laws related to environment are not effectively implemented or lack of awareness. Out of all the species all kinds of damage to our natural environment is caused by only one single species that is homo sapiens. We must accept that environmental crimes have multiple dimensions and it will adversely affect our natural environment and sustainable development goals. Every nation should implement a comprehensive plan for tackling environmental crimes. All countries should support UNEP as the global environmental authority to address the serious and rising environmental impacts of environmental crime.

The damage caused by humans to environment is a crime against humanity because they are harming themselves and their coming future generations. There is a need for strict laws which can control, stop and prevent various kinds of damages to environment. We all are collectively responsible for this loss because some are causing this damage and some are not stopping this damage. By killing animals and trees we humans are welcoming our own end. Rise in sea level, global warming, frequent droughts, vanishing of rivers, extreme weathers etc. all are because of human beings. Strict and effective environmental laws are need of the hour which will serve as a means of legal action for acts that damage or pollute the environment and natural resources.

## **Conclusion**

Man is rapping the nature. Humans are exploiting nature for making their life comfortable. This paper was focused on crime against environment and this must be consider as crime against humanity. It is also a kind of genocide in which humans have completely wiped out some species from this earth and some are going to extinct in future if proper care is not given and some are endangered species. Humans have damaged our earth beyond its capacity to regenerate itself. We, humans have used natural resources in such a huge quantity in just few centuries for fulfilling our material wants which can not be made available in future because it is beyond the producing capacityof earth. We are not only used natural resources extensively but also polluted it. Crime against environment are the acts that cause damage to our natural environment and consequently human health. Good human health is a human right for all people. People have the right to enjoy safe and unpolluted environment and this should be ensure by government. Environment provided and fulfilled each and every basic needs of all humans but we in return caused damage to our natural environment. The environment does not need human beings for its existence but we, humans need environment for our survival. We can't imagine our life without natural environment.

**“The Earth has enough for everyone’s need but not for everyone’s greed”**

- Mahatma Gandhi

## Bibliography

1. Lal's Encyclopaedia on Environment Protection and Pollution Laws, 6<sup>th</sup> Ed. Volume 1, 2 and 3.
2. Justice M.R. Mallick. Environment & Pollution Laws, Professional Book Publishers.
3. KVS Madaan. NTA UGC NET/SET/JRF Paper 1 Teaching and Research Aptitude; 3<sup>rd</sup> Ed. Pearson Publication, Chapter 9
4. <https://www.impactlaw.com/criminal-law/white-collar/environmental-law-violations>
5. [https://www.academia.edu/49252885/CRIME\\_AGAINST\\_ENVIRONMENTAL\\_LAW\\_IN\\_INDIA](https://www.academia.edu/49252885/CRIME_AGAINST_ENVIRONMENTAL_LAW_IN_INDIA)
6. <https://www.cbd.int/financial/monterreytradetech/unep-illegaltrade.pdf>
7. [https://www.unodc.org/documents/NGO/EIA\\_Ecocrime\\_report\\_0908\\_final\\_draft\\_low.pdf](https://www.unodc.org/documents/NGO/EIA_Ecocrime_report_0908_final_draft_low.pdf)
8. <https://www.pdfdrive.com/the-geography-of-environmental-crime-conservation-wildlife-crime-and-environmental-activism-d176077231.html>
9. [https://ec.europa.eu/environment/archives/docum/pdf/02544\\_environmental\\_crime\\_workshop.pdf](https://ec.europa.eu/environment/archives/docum/pdf/02544_environmental_crime_workshop.pdf)
10. [https://wedocs.unep.org/bitstream/handle/20.500.11822/7662/-The\\_rise\\_of\\_environmental\\_crime\\_A\\_growing\\_threat\\_to\\_natural\\_resources\\_peace%2C\\_development\\_and\\_security-2016environmental\\_crimes.pdf.pdf?sequence=3&isAllowed=y](https://wedocs.unep.org/bitstream/handle/20.500.11822/7662/-The_rise_of_environmental_crime_A_growing_threat_to_natural_resources_peace%2C_development_and_security-2016environmental_crimes.pdf.pdf?sequence=3&isAllowed=y)
11. <https://www.scitepress.org/Papers/2018/100941/100941.pdf>

# THE LEGISLATIVE FRAMEWORK FOR PREVENTION OF DIGITAL RAPE IN INDIA: A CRITICAL STUDY

*Manojkumar J. Naik,*

## **Abstract**

Rape is a very loathsome criminal offence. This legal term is coined in order to protect women from imposition of simple words causing more odious and shameful feeling of victimization. Digital rape is the term used to classify offence of rape to differentiate it from other acts of rape causing sexual violence by insertion of any physical object. Before 2013, there was no law to punish offenders of digital rape in India. Different forms of sexual violence injuring mind, body and sexual parts of victim were not defined and therefore not covered by the prevailing criminal laws in India requires to reconsider the law as well as the penal provisions for causing deterrence and thereby prevention and control of such newly emerged actions of accused.

These lacunae in the existing criminal laws causes failure of convicting the accused for their barbaric acts committed against any person irrespective of their age and gender. Other notable thing in offence of rape is only in 1% of cases offence is committed by the strangers. Digital rape is an outcome of today's digital era where information is shared and available on the click with fingertip. In this present scenario author tries to critically analyse the present criminal legislative framework and attempts to suggest effective changes to overcome these emerged and further emerging crimes of sexual violence.

**Keywords:** Digital rape, Sexual violence, physical object, penalization

## **Introduction:**

Gender-based crime, especially against women, is not a new and emerging socio-legal issue. Rape is a very heinous crime. This legal term was created to protect women from the imposition of simple words that lead to more horrible and shameful feelings of victimization. According to the NCRB's 2021 report, crimes against women fell from 56.5% to 64.5%. In India, 428,278 crimes against women were recorded, of which a total of 31,677 rapes were recorded, with an average of 86 complaints per day and 49 crimes recorded per hour in 2021. Rajasthan (6,337) tops list, followed by Madhya Pradesh (2,947), Maharashtra (2,496), Uttar Pradesh (2,845) and Delhi with 1,250

recorded rapes in 2021. Digital rape is the term used to classify the crime of rape in order to distinguish it from other rapes. This results in sexual violence through the penetration of any physical object. "Digital Rape" became a national sensation. We can therefore assume that the word "digital" is related to the word "rape" in the digital world. However, digital rape has nothing to do with gadgets such as computers, phones, laptops, or platforms owned by Meta.

The word is derived from the English word "digit", which literally means number and whole number. Also, the word means a finger or a toe. The term digital rape is neutral and applies to all types of victims and perpetrators. Rape victims are further divided into two categories: primary and minor. There are two types of rapists who commit crimes: small digital rapists and large digital rapists. A person who commits such an offense is liable to a fine of Rs 50,000 under Sections 5 and 6 of the POCSO Act.

Under the terms of article 3 of the POCSO law, "Any person who undertakes to insert an object or a part of the body (other than a penis) into the vagina, urethra or anus of a child, or of a child doing so with him or any other person is considered penetrating sexual assault. The laws regarding digital rape came into effect after 2012. Until now, there was no mention of digital rape in the Indian Penal Code (IPC). Previously, this fell under the classification of harassment rather than rape.

It has been reported that in 70% of cases, the person who violated the dignity of a woman or a child was an acquaintance. The crimes were committed by close relatives of the victims. In 29% of cases, the aggressor came from the victim's social circle, and in only 1% of cases, the aggressor was a complete stranger.

### **Meaning of the term Rape in criminal law?**

Article 375 of the ICC defines rape as "without a woman's consent, by duress, misrepresentation or fraud, or while she is intoxicated, 18 years of age." This heinous crime breaks down into several types; let's take a look at them.

### **Types of Rape**

**Date Rape** - The term 'acquaintance rape' is widely known as 'acquaintance rape', i.e. non-domestic rape perpetrated by a known person of the victim. It is a drug-induced sexual assault in which the rapist intentionally drugs the victim with date rape drugs to incapacitate her. The most common example is adding water to the victim's drink.

**Gang Rape** - This is when a group of people participate in the rape of a single victim. Rape involving two or more perpetrators is widely reported in many parts of the world. Section 376(2)(g) sets out the penalties for gang rape. It stipulates that offenders will be punished with a harsh prison sentence of at least ten years, up to life imprisonment, and a fine or both. Gang rape cases that have angered

the public include the Nirbhaya rape case and the Bilkis Bano gang rape case.

**Marital rape** - This type of rape is also called marital rape and is rape between married or common-law partners without the consent of either spouse. Marital rape is considered a form of domestic violence and sexual abuse. Exception 2 of Section 375 prevents the passage or recognition of this marital rape law because it states that "a man who has sexual intercourse or a sexual act with his own wife, while the wife has under 15, does not violate is not", in some cases the courts have set it at 18 instead of 15.

**Child rape** - This is a form of child sexual abuse. When another child (usually older or stronger) or a teenager commits a sexual assault, it is called child-to-child sexual abuse. POCSO is the law that regulates child sexual abuse.

**Custodial Rape**- Section 376A states that rape is custodial rape when committed by a male while the female is in custody. These people can call any policeman, constable, etc., Detain the woman. It would be a very heinous crime if they abused their power to sexually exploit women. However, in 1983 the concept took on new meaning and the meaning of the word "conservation" was broadened. A popular example is the rape of Mathura.

**Digital rape**- In this offence of rape, accused is using the forced insertion of fingers and toes without the consent of the victim and is not related to cybercrime. Let us understand this form of rape in detail. Digital rape is the term used to classify the crime of rape to distinguish it from other rapes. This results in sexual violence through the penetration of any physical object.

### **What does digital rape mean?**

In digital rape, the perpetrator uses one or more of his fingers or any other tangible object to rape and force a sexual act on the victim. In a nutshell, a person is accused of digital rape when the abuser uses one or more of his fingers or any other physical object to penetrate the victim's vagina without the victim's consent. Some Reported Incidents of Digital Rape in India -

*Incident 1* - In a very outrageous incident, a bleeding 2-year-old girl in Mumbai was taken to hospital where doctors discovered that her vagina had ruptured. However, there was no evidence of sexual abuse or rape. However, it was later discovered that her father fingered the girl. He was arrested but punished under article 376 of the CPI.

*Incident 2* - Then, in another incident, a 60-year-old woman was sexually assaulted by a tricycle driver who penetrated her body with an iron rod while attending a relative's wedding. The driver was again arrested but not convicted under Article 376 of the CPI, pointing out several shortcomings of Article 376 of the CPI.



*Incident 3-* The Nirbhaya case cannot be ignored when talking about digital rape, in this case the victim was again gang raped and one of the underage defendants inserted an iron rod into the vagina of the victim and the doctor reported that she had nothing left of her intestines 5% abdomen.

As he points out several shortcomings in article 376 of the ICC, which deals with the punishment of the crime of rape, because digital rape involves the violation of a woman's dignity using a finger, foreign object or any other part of the shredded cheese. But after the Criminal Amendment Act of 2013, the Supreme Court had to make some changes to its definition of rape in the IPC. With all these heinous cases and crimes in mind, the definition of rape was expanded in 2013. With this new definition, rape is now defined as "the insertion of a penis, any foreign object or any other part of the body in a woman's vagina, mouth, anus or urethra".

### **What are the penalties for cyber rape?**

IPC Law and POCSO state the penalties for various rape offenses. Under the POCSO law, offenders will be sentenced to five years in prison, which can be extended from 10 years to life imprisonment if it falls under Article 376 of the IPC. The provisions dealing with penalties under the POCSO are as follows:

**Section 3** of the POCSO Act Although changes were made to the definition of rape under Section 376 of the ICC in 2013, penetration of any object other than the penis to "any extent" is subject to Section 3 of the POCSO Act. or any part of the body in the vagina, urethra or anus of a child, or a child provokes such an act on himself or any other person was considered penetrative sexual assault. digital rape, not only these two clauses are considered POCSO Act

**Section 5 (m)** and Section 6. While Section 3 defines penetrative sexual assault, Section 5 of the POCSO Act defines seriousness Penetration aggravated penetrative sexual assault ranges from 20 years criminal imprisonment to life imprisonment (including any natural life sentence) or even death, with an additional sentence.

**Section 6 (1)** Anyone who commits sexual assault with aggravated penetration shall be punished with a term of imprisonment of at least 20 years, which may go as far as life imprisonment, i.e. imprisonment for life. conduct of the person and will be punished with a fine or the death penalty. A fine imposed under subsection (1) must be just and reasonable and payable to the victim to cover his medical and rehabilitation expenses. The term "woman" in Article 375 of the IPC has been replaced with a person, and the article is now amended to be gender neutral to include sexual offenses committed against any person, regardless of gender.

**Section 375A-** Sexual Assault and Penalties for Sexual Assault-- "(1) The following constitutes

sexual assault if a person: - (a) intentionally touches the person's genitals, anus, or breasts, or the person touches the person's genitals, Anal touching the vagina, penis, anus, or breasts of that person or any other person without that person's consent, unless such contact is for appropriate health or medical purposes; (b) Use of another person's words, gestures, or gestures that make an unwelcome actionable sexual threat or induce unwelcome advances; and shall be punished with imprisonment for up to three years, or a fine, or both. Explanations 1. "For the purposes of this section, the term genital refers to the penis and the vagina; "vagina" also includes the labia majora. Explanation 2. "Consent is an express voluntary agreement when an individual expresses, by words, gestures or any form of non-verbal communication, his or her willingness to engage in a particular act. Explanation 3. For the purposes of this article, the term touching means sexual contact without the consent of the victim and without reasonable grounds to believe that the victim has consented.

## **Rape Laws in India**

Apart from the POCSO and IPC laws, the following provisions can be generalized to deal with the crime of rape in India. IPC U/s 228A[2], No one shall give the name of a victim of rape, and if anyone does, he will be punished by any description, the sentence may be extended to two years, and it will be liable to a fine. U/s 114-A [3] Indian Evidence Act, non-consent may be presumed in some rape prosecutions. U/s 53(1)(4), where a person is arrested for committing an offense of this nature which is alleged to have been committed in circumstances where there were reasonable grounds to believe that the questioning against him produce evidence of a crime, a licensed physician acting at the request of a police officer not below the rank of sub-inspector and any person acting in good faith with the aid of him and under his direction to make reasonable claims against the arrested person in order to determine the facts that such evidence may provide and to prevent the use of violence reasonably necessary for this purpose. U/s 164A[5] of the CPR sets out rules for the medical examination of rape victims. U/s 327(2)(6) of the CRPC, all rape victims must be tried in secret.

## **Conclusion**

There is an urgent need to change India's rape laws following the Nirbhaya rape. Prior to 2013, digital rape was not included in the definition of rape. But after several heinous rapes, as mentioned above, the legislator and the judiciary felt the need to make many changes to the definition of rape, knowing that there are other ways a man can use to violate the dignity of a woman or a child. So, keeping all these cases and heinous crimes, the definition of rape was expanded in 2013 and rape is now defined

as "the insertion of a penis, any foreign object or any other part of the vagina, a woman's mouth, anus or urethra", and severe punishment for such a heinous crime.

## **References**

Laws-in-India-Appropriate-or-Not?.html on 01/22/2023

2. Retrieved from [https://www.livelaw.in/pdf\\_upload/pdf\\_upload-362124.pdf](https://www.livelaw.in/pdf_upload/pdf_upload-362124.pdf) on 2023-02-10

3. Retrieved from [https://www.mha.gov.in/sites/default/files/2022-](https://www.mha.gov.in/sites/default/files/2022-08/CSdivTheCriminalLawAct_14082018%5B1%5D.pdf)

08/CSdivTheCriminalLawAct\_14082018%5B1%5D.pdf 2023-02-10

4. See Ratanlal and Dhirajlal, Indian Penal Code, 1860, 10th Edition, Eastern Publication House, 2004

5. See Indian Evidence Act, 1872

6. See Criminal Procedure Code, 1973

## **BISEXUALITY IN MODERN SOCIETY**

- Samruddhi R. Patil
- Aditya S. Deshmukh

### **Abstract**

There are many different subgroups within the lesbian, gay, bisexual, and transgender (LGBT) community, including groupings based on sexual orientation and/or gender identity, but it's unclear whether the modern world recognises distinctions in how they view these groups. If so, what circumstances lead people to judge homosexual, bisexuals and transgender people differently? This study analyses the changing sentiments about these communities through a legal perspective. The studies show that variations in these mindsets that are related to social contact effects, variations in cognitive consistency, social cues, and the changing degrees of important political characteristics like affiliation and religion.

**Keywords:** transgender, bisexuality LGBT, public opinion, interpersonal contact, group

### **Introduction**

Homosexuality is seen as the middle ground between "normal" orientation and inversion, and it sits in the middle of the polarity between sexes, roles, and sexual goals. Homosexuality is defined as the inversion of gender/sexual characteristics on a heteronormative scale. Bisexuality, according to Sedgwick, challenges the reversed heteronormative schema, which pits homosexuality, which is represented as having opposite-sex desires, against heterosexuality. (same-sex desire). This claim states that bisexuality is a bridge between heterosexual and homosexual orientations, which calls into doubt the validity of the heteronormativity arguments made by this opposition.

Despite significant ideas and research on bisexuality, as well as an increasing knowledge and acceptance of LGBTIQ sexuality in many Western nations, bisexuality still carries a lot of stigma. The persistence of a heterosexual/homosexual binary sexuality model, in which there are only two varieties of sexual identity, attests to the obscurity of bisexuality. Unisexuality, the propensity to highlight the same-sex appeals and/or sexual behaviour of gay, lesbian, and straight people, furthers bisexual invisibility. The everyday structure of sexuality, as well as how sexuality is portrayed in the media and popular culture, are all dominated by the binary of sexuality and unisexism.

Recent years have seen a significant shift in the public's perception of heterosexual behavior, and the same is now true of bisexuality, which is now preferred to homosexuality because it more accurately conveys the idea that complete restriction of all behaviour cannot be considered the norm.

### **Research objectives**

- To understand the concept of bisexuality, its historical presence and societal status.
- To study various interpretation of the bisexuality in society.
- To deliberate on the issue of social acceptance of bisexuality in modern society.

### **Research Question**

- What makes bisexuality different?
- How is bisexuality an inevitable part of the modern society?
- What is the status of bisexuality in contemporary India?

### **Research Methodology-**

To make sure that all of the subject's antecedents and origins are thoroughly investigated, a didactic research approach is applied. Secondary material must be researched and studied when conducting academic research, especially in the beginning. The majority of their time is spent looking for and analyzing the materials utilized to create the project's concept and design as well as reading and researching numerous pieces of literature that are connected. A legal definition and synthesis of the analysis of the complete text are required in order to determine whether a text is truthful. Nearly all of the data collected for this study were unintentional or secondary. There is no primary research conducted; the majority of the data is gathered from secondary sources. Various materials such as books, articles and magazines were used in the development of the project.

### **Analysis**

#### **I. Understanding bisexuality**

One who exhibits emotional, romantic, and/or sexual attraction to, or engages in romantic or sexual relationships with, more than one gender or sex is referred to as bisexual. Bisexuality is defined by famous bisexual activist and writer Robyn Ochs as "the capacity to experience emotional and/or sexual attraction to more than one person of the same sex, not necessarily at the

same time, not necessarily in the same way, and not necessarily in the same way." Even if a person does not identify as bisexual, bisexual orientation might still exist. According to a 2016 article by the Centers for Disease Control and Prevention, 1.3% of women and 1.9% of men describe themselves as "gay, gay, or lesbian," and 5.5% of women and 2% of men describe themselves as "bisexual." According to these results, the LGB community for women and men may be predominantly bisexual.

Gender minority labels are dynamic, diversified, and culturally different. Some often used terminology include lesbian, gay, bi (pronounced "bi plus"), queer, and asexual, but this list is not exhaustive. Within the group, there are additional variances. The bi community, for instance, includes those who identify as bisexual, fluid, bisexual, or bisexual. Significant differences also exist among other gender minority groups. Attempts to attain marriage equality, for instance, have come under fire for failing to sufficiently address the worries of people who identify as bisexual and gender nonconforming (bi). (Marcus, 2018). The phrase "eliminating bisexuals" alludes to the uncertainty that two persons must experience even in groups that defend sexual minorities.

## **II. Paradigm of gender identity and sexual orientation**

Gender minority labels are dynamic, diversified, and culturally different. Some often used terminology include lesbian, gay, bi (pronounced "bi plus"), queer, and asexual, but this list is not exhaustive. Within the group, there are additional variances. The bi community, for instance, includes those who identify as bisexual, fluid, bisexual, or bisexual. Significant differences also exist among other gender minority groups. Attempts to attain marriage equality, for instance, have come under fire for failing to sufficiently address the worries of people who identify as bisexual and gender nonconforming (bi). (Marcus, 2018). The phrase "eliminating bisexuals" alludes to the uncertainty that two persons must experience even in groups that defend sexual minorities.

However, sexual orientation describes a person's ongoing desire for, and attraction to, other people, including those who are transgender or who have alternative gender identities. Sexual orientation, which includes heterosexuality, bisexuality, asexuality, and other classifications, may or may not change during or after gender transition. The way that a person identifies as sexually (or otherwise, such as asexual or, in the case of modern sapiosexuals, sexually) attracted to others is known as their sexual orientation. Being straight or homosexual, for instance. - It is not possible to categorise someone's sexual orientation as either homosexual or heterosexual. A

person might identify with a number of distinct trends. An individual might identify as gay, straight, bisexual, asexual, pansexual, or polysexual, for instance.

The "gender or sexes" that they target are referred to as this "identity." Speaking of which, "gender" is a rather broad phrase. Gender can either be defined in a biological sense, such as a person's sex, masculinity, or femininity, depending on the situation, or it can be defined in terms of the social and cultural structures of the society in which a person lives. Each person's self-defined gender identity and gender identity are key components of their personality and of the right to self-determination, human dignity, and freedom. Gender identity and gender identity are distinct notions. No one may be compelled to undergo medical procedures like gender reassignment surgery, sterilization, or hormone therapy as a condition of having their gender identity legally recognised<sup>1</sup>.

### **III. Disparities in health among bisexual people**

Within the LGBTQ community, those who identify as bisexual make up the largest identity group. A physical, romantic, or sexual attraction that is not specific to one sex or gender is known as bisexuality. Bisexuality encompasses a wide range of sexual orientations, hence there are many different ways to identify as bisexual. Bisexuality is the term used to describe a person's attraction to both men and women. Others may define it as an attraction to a gender that is both similar to and different from their own, or as an attraction to gender in general.

Bisexuality is becoming more prevalent, with nearly 12% of Gen Z adults (ages 18–23) identifying as bisexual, but it's still a sexuality that's widely misunderstood and stereotyped. When compared to gay, lesbian, and straight people, bisexuals who experience stigma and prejudice may experience exclusion, isolation, and lower health outcomes.

When you first become aware of your sexuality, you may be aware that you are neither straight nor homosexual, but you may not be aware that bisexuality is a sexual orientation or that there are terminology for what you are going through. Many bisexual people report that they do not always experience the same level of attraction to multiple genders. It may cause you to question your attraction to a particular gender and make you wonder whether you are homosexual or straight rather than bisexual.

Bisexuals have startlingly poor health, including issues with cancer, obesity, STDs, and mental health. Bisexuals are the largest group in the LGBT community, according to research, making up about half of all those who identify as lesbian, gay, or bisexual. Despite this, the LGBT community

does little to meet the needs of bisexuals. More than 40% of LGBT people of colour identify as bisexual, and roughly 50% of transgender people describe their sexual orientation as bisexual or queer. These statistics make the bisexual community, as well as transgender people and people of color, particularly vulnerable to new forms of segregation that emerge at the intersection of biphobia, racism, and transphobia. Bisexual people who have had negative encounters with healthcare may postpone appointments, switch healthcare organizations, conceal their sexual orientation in subsequent meetings with healthcare professionals, and turn to online resources for health advice rather than medical professionals.

#### **IV. Bisexual erasure**

Bisexual invisibility is another name for bisexual erasure. As the phrase implies, to fake, disregard, or reject the sexual orientation of bisexuality is to erase bisexuality. Many people have misconceptions about what being bisexual implies, believing that it is only a passing phase that will be replaced by homosexuality or heterosexuality, or, to put it more simply, that those who "come out" as bisexual would quickly switch to the opposite side. This in itself is a problem since people who identify as bisexual are put under a lot of strain because of the widespread societal idea that they will be erased. One explanation could be that bisexuality is stigmatised in both homosexual and LGBT communities in addition to straight communities. Biphobia is a syndrome that has emerged as a result of this widespread social stigma. Biphobia is the derogatory term for ignorance or hostility towards bisexuality. Bisexuals may be subjected to prejudice as a result of this, which can range from denial of bisexuality to intolerance or hatred of the existence of bisexuals.

According to statistics, 5.6% of American adults in February 2021 self-identified as homosexual, gay, bisexual, or transgender. 54.6 percent of this group self-identify as bisexual, which is more than half. According to this, 3.1% of all American people self-identify as bisexual. Let's talk about India now. According to the GLOBAL PRIDE 2021 GLOBAL SURVEY, which was carried out by the international firm Ipsos with a sample of roughly 500 persons, 9% of Indians (who identified themselves) identified as bisexual. Due to the social stigma that any identification other than heterosexuality is not considered or, if considered, can be subjected to discrimination or humiliation, many persons misinterpreted this topic or chose to remain silent.

#### **V. Biphobia, crime and violence**



Biphobia refers to detrimental attitudes, behaviors, and social norms that attack people who are attracted to more than one gender. Biphobia is on the rise as a result of how bisexuals are frequently portrayed, and attitudes towards them are frequently even more negative than those towards other minority groups. The term "one-sex privilege," which refers to the privileges received by everyone who is attracted to only one gender, is related to this idea.<sup>28</sup>

## VI. Legal complexities- evidence of dilution of bisexuality

It goes without saying that since **Inc. v. Olesen in 1958**, which laid the groundwork for successful anti-discrimination lawsuits for the LGBT community, courts have been busy issuing rulings to end discrimination based on a person's sexual orientation. However, bisexual erasure has also filtered into them.

At the **Bostock v. The US Supreme Court** used the terms "gay," "homosexual," or "transgender" in its ruling in Clayton County, one of the most significant decisions to outlaw job discrimination based on sexual orientation. For many who identify as bisexual, the fact that the courts themselves do not use the term "bisexual" in their rulings is a genuine worry. One of the dangers of the Bostock decision was that, because the term "bisexual" was not used, we can only infer that the courts intended to apply it to all sexual orientations, not only "gay" or "transgender," since they did not specifically specify it. It could be important to avoid reading the judgement literally in light of this. The fact that the Second Circuit did not define a particular term in **Bostock, Zarda v. Altitude Express, Inc.**, one case, gives us some solace.

The circumstances in *Romer v. Evans* were comparable. Even though the ruling caused a lot of controversy, it can be seen as an instance of bisexual erasure since the judges only specifically addressed "homosexuals or gays or lesbians." These case laws serve as a few illustrations of how bisexual erasure has slipped through the legal system's crevices.

### In India

In India, LGBT rights have been developing. The stigma surrounding the subject is still very much alive, though. Although more and more people are accepting of their sexual orientation, a sizeable

---

<sup>28</sup> Barker, Meg; Richards, Christina; Jones, Rebecca; Bowes-Catton, Helen; Plowman, Tracey; Yockney, Jen and Morgan, Marcus (2012). *The Bisexuality Report: Bisexual inclusion in LGBT equality and diversity*. Centre for Citizenship, Identity and Governance. The Open University.

portion of the population is still either unaware of it or actively denies it. The problem of ignorance is sometimes accompanied by mocking, which significantly worsens the circumstance.

Similarly to the enormous roller coaster that started in **Naz Foundation v. Govt. of NCT** of Delhi in 2009, continued with **Suresh Kumar Koushal v. Naz Foundation**, and culminated in **Navtej Singh Johar and Ors.** in the year Union of India. The Ministry of Law and Justice of India has witnessed numerous legal viewpoints and interpretations with regard to Section 377 of the Indian Penal Code. Oral sex between two adults of the same sex does not contravene Article 377 and is a component of the fundamental rights guaranteed by the Indian Constitution, the Hon'ble High Court said in 2009. In the case of *Suresh Kumar Koushal v. Foundation Naz*, the Supreme Court overturned the judgment in 2013. Ultimately, in 2018, the Hon'ble Supreme Court of India decriminalized consensual intercourse between legal-age adults in *Navtej Singh Johar & Ors. v. Union of India*.

As seen in these cases from India, there is still some evidence of bisexual erasure. We can only assume that all sexual orientations are treated equally by the decisions. The court found that Section 377 of the Indian Penal Code only decriminalised same-sex intercourse as the rationale for this.

## **Conclusion**

Compassion, feeling, the capacity to comprehend your own issues, and empathy are a few of the most important enablers. It seems to me that by eliminating bisexuals, we would be losing a crucial aspect of what makes us human—compassion. Many people are now being subjected to this egregious negligence, which is imposed upon them either purposefully or due to ignorance. A "disease" cannot be bisexuality. Not a "phase" or "transition," either. As real as it gets, this is. I mentioned the data, or the actual percentage of bisexuals, earlier in the text. Remember that only people who have demonstrated incredible bravery and self-acceptance in the face of social stigma are included in this list.

Bisexual deletion, often known as bi-deletion, affects many people's mental health. The deliberate omission of sexual orientation has been linked to numerous mental health issues. Due to the growing scorn for or disregard for bisexuality, people experienced despair, anxiety, and other behavioral disorders. A person's sexuality is something private and in some ways contributes to their definition. Why not permit individuals to identify themselves whenever and however they, please? Encouraging others to come forward and put an end to this social stigma requires just enough. Put an end to double erasing and strive for a brighter future.

## Webliography

- American Psychological Association. (2021). Bisexuality. Retrieved from <https://www.apa.org/topics/bisexuality>
- Human Rights Campaign. (n.d.). Bisexuality. Retrieved from <https://www.hrc.org/resources/bisexual-issues>
- Bisexual Resource Center. (n.d.). About bisexuality. Retrieved from <https://biresource.org/bisexuality/>
- GLAAD. (n.d.). Bisexual resources. Retrieved from <https://www.glaad.org/bisexual/resources>
- Bisexual.org. (n.d.). Bisexuality 101. Retrieved from <https://bisexual.org/bisexuality-101/>
- National Center for Transgender Equality. (n.d.). Bisexuality. Retrieved from <https://transequality.org/issues/bisexuality>
- Planned Parenthood. (n.d.). Bisexuality. Retrieved from <https://www.plannedparenthood.org/learn/sexual-orientation/bisexuality>
- The Trevor Project. (n.d.). Bisexuality. Retrieved from [https://www.thetrevorproject.org/trvr\\_support\\_center/bisexuality/](https://www.thetrevorproject.org/trvr_support_center/bisexuality/)

## CYBER TERRORISM AND LAW

-Ramashankar Dasharath Singh

### **Abstract**

Cyber terrorism refers to the use of technology to commit acts of terror and violence against individuals, organizations, or governments. With the rise of the internet and digital technology, cyberterrorism has become a growing concern for law enforcement and security agencies. The purpose of this article is to examine the issue of cyberterrorism and the laws surrounding it. The internet has created a new arena for terrorists to operate, allowing them to remain anonymous and evade detection. Cyberterrorists use various tactics such as website defacement, denial of service attacks, and malware to spread fear and cause harm. These attacks can cause significant damage to critical infrastructure, steal sensitive information, or even disrupt entire economies. In response to the threat of cyberterrorism, governments around the world have introduced laws and regulations aimed at preventing and combating these crimes. The United States has enacted the Computer Fraud and Abuse Act (CFAA) to criminalize unauthorized access to protected computer systems and the theft of confidential information. Additionally, the Electronic Communications Privacy Act (ECPA) provides for the interception of electronic communications for law enforcement purposes. Similarly, the European Union has enacted the Network and Information Systems Directive (NISD) to ensure the security of critical infrastructure, including the protection of networks and systems against cyberattacks. The NISD also requires organizations to report incidents of cybercrime to the relevant authorities. International law has also played a role in addressing cyberterrorism. The Council of Europe Convention on Cybercrime aims to provide a harmonized approach to addressing cybercrime and cyberterrorism, including the suppression of illegal activities and the protection of privacy and personal data. The United Nations also has a number of initiatives aimed at promoting the peaceful use of information and communication technologies and preventing their abuse for malicious purposes. The need for effective laws to address cyberterrorism is becoming increasingly pressing as the number of incidents continues to rise, and it is important for governments and international organizations to work together to develop a comprehensive approach to this threat.

**Keywords:** cybercrime, criminalize, cyberterrorism, malicious, government.

## **Introduction:**

Cyberterrorism is a relatively new phenomenon that has emerged with the advancement of technology and the increasing reliance on digital systems and networks. It refers to the use of the internet and other forms of technology for the purpose of promoting and perpetrating acts of terrorism. The use of technology in this way presents a unique set of challenges and concerns, both in terms of the potential impact on society and the difficulties in preventing and responding to cyberattacks. Cyberterrorism can take many forms, including the spread of propaganda and recruitment efforts, the theft of sensitive information and the use of malware to disrupt critical infrastructure and essential services. The consequences of cyberterrorism can be far-reaching, with the potential to cause widespread disruption, loss of life, and economic damage.

In response to the threat of cyberterrorism, national governments and international organizations have developed a range of laws and regulations to address the issue. The development of these laws and regulations has been a slow and evolving process, as the law has struggled to keep pace with the rapid advancements in technology. However, there have been significant developments in recent years, and many countries now have specific legislation in place to address cybercrime, including cyberterrorism. One of the key challenges in developing laws and regulations to address cyberterrorism is the nature of the internet itself. The internet is a global network, which means that cyberattacks can originate from anywhere in the world and target anyone, anywhere. This makes it difficult for national governments to respond effectively to cyberattacks, and raises questions about jurisdiction and the extent to which different countries should be responsible for regulating the internet.

Another challenge in addressing cyberterrorism is the need to balance security and privacy. While it is important to have measures in place to prevent and respond to cyberattacks, it is also important to ensure that these measures do not infringe on the rights and freedoms of individuals. This requires a careful balancing of interests, and the development of laws and regulations that are both effective and respect the rights of citizens.

The laws and regulations that have been developed to address cyberterrorism can be grouped into several categories, including:

Laws and regulations that deal with the actual commission of cyberattacks, including the theft of sensitive information, the spread of malware and the disruption of critical infrastructure.

Laws and regulations that deal with the dissemination of propaganda and recruitment efforts by terrorists, including the use of the internet and social media for these purposes.

Laws and regulations that deal with the activities of individuals and organizations that support cyberterrorism, including the provision of funding, the development of malware, and the hosting of websites and other resources used by terrorists.

Laws and regulations that deal with the role of service providers and technology companies in preventing and responding to cyberattacks.

International agreements and treaties that set standards for the exchange of information and cooperation between countries in the fight against cyberterrorism.

The threat of cyberterrorism is a significant concern for national governments and international organizations. The development of laws and regulations to address this threat is an ongoing process, and requires a careful balancing of security and privacy.

### **Meaning:**

Cyber terrorism is defined as unlawful attacks and threats against computers, networks, and information stored on them in order to intimidate or coerce a government or its people in furtherance of some political or social goals.

Merriam Webster defines Cyberterrorism as “*terrorist activities intended to damage or disrupt vital computer systems*”.<sup>1</sup>

<sup>1</sup> Cyberterrorism Definition & Meaning - Merriam-Webster,

<https://www.merriam-webster.com/dictionary/cyberterrorism> (last visited Feb 13, 2023).

While the Cambridge Dictionary defines it as *“the use of the internet to damage or destroy computer systems for political or other reasons”*.<sup>2</sup>

Cyberterrorism is a global threat that requires a coordinated international response. The lack of clear international legal frameworks and the cross-border nature of digital attacks make it difficult for governments to effectively combat cyberterrorism. In many cases, the perpetrators of cyberattacks are difficult to identify, and the complexity of digital networks and the speed at which they can spread malware make it challenging to respond in a timely manner. To address the challenges posed by cyberterrorism, many countries have enacted laws to protect against digital attacks. These laws typically focus on protecting critical infrastructure, providing law enforcement with the necessary powers to combat cybercrime, and establishing legal frameworks for the prosecution of cybercriminals.

### **Research Objectives:**

The objective of writing this paper is to elaborately research on the field of cybercrime and cyberterrorism. Get insights on cyberterrorism in India and its legal ramifications. Highlight upon the initiatives taken by the international community and our country to combat cyberterrorism.

### **Hypothesis**

Cyber terrorism is on the rise as a result of the government's policies and laws, so we must tighten our security systems, policies, initiatives, and punishments to combat it.

### **Methodology:**

The research design adopted for this study is qualitative research design. Qualitative research is appropriate for this study as it enables an in-depth exploration of the complex and multifaceted nature of cyberterrorism.

---

<sup>2</sup> CYBERTERRORISM | English meaning - Cambridge Dictionary, <https://dictionary.cambridge.org/dictionary/english/cyberterrorism> (last visited Feb 13, 2023).

## Scope of Cyberterrorism

Cyberterrorism refers to the use of digital technology and the internet for the purpose of perpetrating terror or inciting fear in a population. In recent years, cyberterrorism has become a growing threat to the global community, and India is no exception. India has a rapidly growing economy that is highly dependent on digital technology, and as such, the country is particularly vulnerable to cyberattacks that could impact its economy, social stability, and national security.

The scope of cyberterrorism in India has become increasingly broad in recent years, with the country experiencing a range of cyberattacks that have caused widespread disruption and damage. One of the most notable forms of cyberterrorism in India has been the use of ransomware attacks. **Ransomware attacks** are a type of cyberattack that encrypts a victim's data and demands payment in exchange for the decryption key. These types of attacks have become increasingly common in India and have targeted a range of organizations, including government agencies, businesses, and educational institutions.

Another form of cyberterrorism that has become prevalent in India is phishing attacks. **Phishing attacks** are designed to trick victims into disclosing sensitive information, such as passwords and bank account details, by sending emails or messages that appear to be from a trustworthy source. These attacks are often used to steal sensitive information or to spread malware. In India, phishing attacks have become increasingly common and have targeted a range of organizations and individuals, including government employees and private sector employees.

The scope of cyberterrorism in India also extends to the use of social media platforms for the spread of false or misleading information. The use of social media has become a powerful tool for extremists and terrorists to spread propaganda, incite fear, and mobilize support for their causes. In India, the use of social media to spread false or misleading information has become a major concern, particularly during periods of social unrest or political turmoil.

In addition to the above-mentioned forms of cyberterrorism, India has also faced a range of other cyberattacks, including denial of service (**DDoS**) attacks, **malware attacks**, and **data breaches**. These attacks have impacted a range of organizations and individuals and have caused widespread disruption, damage, and loss of sensitive information. In response to these threats, the Indian government has taken a number of steps to enhance the country's cybersecurity,



including the establishment of a **National Cybersecurity Coordination Centre (NCCC)** and the development of a **National Cybersecurity Policy**.

**Check Point Research (CPR)**<sup>3</sup> released new data on 2022 cyber attack trends showing that global cyber attacks increased by 38% in 2022, compared to 2021. These cyber attack numbers were driven by smaller, more agile hacker and ransomware gangs, who focused on exploiting collaboration tools used in work-from-home environments, targeting education institutions that shifted to e-learning post COVID-19.

This increase in global cyber-attacks also stems from hacker interest in healthcare organisations, which saw the largest increase in cyber-attacks in 2022, when compared to all other industries. CPR warns that the maturity of **AI technology**, such as **CHATGPT**, can accelerate the number of cyber-attacks in 2023.

Threats posed by cyber terrorism:

**Data Breaches:** Cyber terrorists can break into computer systems, steal sensitive information and cause massive data breaches that put individuals, organizations, and even nations at risk.

**Infrastructure Disruptions:** Cyber terrorism can also result in the disruption of critical infrastructure systems such as power grids, transportation systems, and financial systems, potentially causing widespread harm.

**Financial Losses:** Cyberattacks carried out by terrorists can cause significant financial losses for individuals and organizations, particularly small businesses that may not have the resources to recover.

**Intellectual Property Theft:** Terrorists can also use cyberattacks to steal sensitive intellectual property, putting companies at a disadvantage in the global market.

<sup>3</sup> ET CIO.com SOUTH-EAST ASIA | Report Global Cyber Attacks 2022  
<https://ciosea.economicstimes.indiatimes.com/news/security/global-cyber-attacks-increased-by-38-in-2022-report/96869258> (last visited Feb 13, 2023).

**Reputation Damage:** Cyber terrorism can also cause significant damage to a company's reputation, as news of a breach can spread rapidly and affect public perception.

**Political Instability:** Cyberterrorism can also have political implications, as it can be used to disrupt elections or destabilize governments by leaking sensitive information or launching cyberattacks on government websites.

**Psychological Trauma:** The fear and uncertainty caused by cyber terrorism can have a profound psychological impact on individuals and communities, leading to stress, anxiety, and even post-traumatic stress disorder (PTSD).

**Public Safety Threats:** In some cases, cyber terrorism can also pose a direct threat to public safety, as terrorists could potentially use cyberattacks to target emergency responsesystems or disrupt transportation systems.

**Global Interconnectivity:** With the increasing interconnectivity of global systems, cyber terrorism has the potential to cause widespread harm across national borders, making it a global threat.

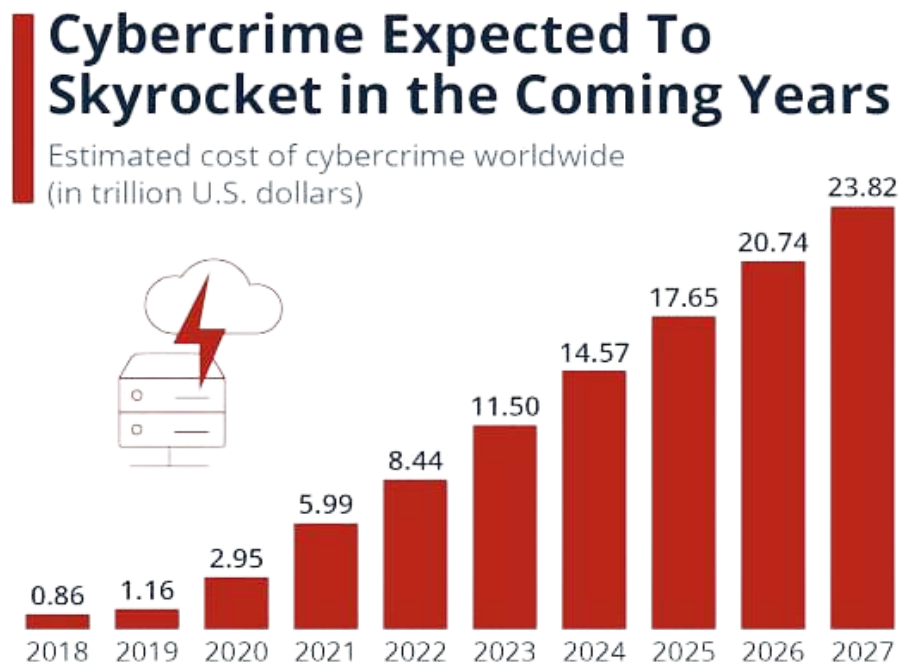
### **Cyber terrorists' potential targets include:**

Cyber terrorism refers to the use of digital technology to carry out acts of terrorism, including cyberattacks on critical infrastructure, websites, and communication networks. As our world becomes increasingly dependent on digital technology, the threat of cyber terrorism continues to grow. One potential target is critical infrastructure, such as power grids, water treatment plants, and transportation systems. A cyberattack on these systems could cause widespread disruption and chaos, potentially leading to widespread power outages, water shortages, or transportation disruptions. For example, a cyberattack on a power grid could result in blackouts and widespreaddisruption of essential services, while a cyberattack on a water treatment plant could contaminatethe water supply, leading to widespread health concerns. Another potential target of cyberterrorism is financial institutions, such as banks and stock exchanges.

This organization hold vast amounts of sensitive financial information and control significant portions of the global economy.

Websites and communication networks are also potential targets of cyber terrorism. A cyberattack on these networks could result in the shutdown of websites, the compromise of sensitive information, or the disruption of communications. For example, a cyberattack on a major social media network could result in the dissemination of false information, causing panic and confusion among the general public.

Finally, government and military organizations are also potential targets of cyber terrorism. A cyberattack on these organizations could compromise sensitive information, disrupt operations, or cause widespread panic and confusion. For example, a cyberattack on a military network could compromise sensitive information and disrupt operations, while a cyberattack on a government website could result in the dissemination of false information, causing widespread panic and confusion. As our world becomes increasingly dependent on digital technology, it is crucial that we take steps to mitigate the threat of cyber terrorism, including implementing robust cyber security measures, improving our ability to respond to cyberattacks, and developing international norms and agreements to govern state behavior in cyberspace.



(Source: Statista Technology Market Outlook, National Cyber Security Organisations, IMF)

## **Cyberspace exploitation**

Cyberspace exploitation refers to the illegal use of computer networks, information technology systems, and the internet to carry out malicious activities such as theft, fraud, and cyber attacks. These activities often result in significant financial losses, damage to reputation and identity, and threat to national security.

One of the most common forms of cyberspace exploitation is hacking, where individuals or groups gain unauthorized access to computer systems, networks, and personal information. Hackers use various techniques to bypass security systems and gain access to sensitive information, such as passwords, financial data, and personal identification. They then use this information for malicious purposes, such as identity theft, financial fraud, and data manipulation.

Another form of cyberspace exploitation is phishing, where individuals or groups send emails or messages that appear to be from legitimate sources, such as banks, retailers, or government agencies, to trick individuals into revealing their personal information or downloading malware onto their computer.

Cyberspace exploitation also includes the use of malware, such as viruses, Trojans, and spyware, which can infect computers and cause significant harm to individuals, organizations, and entire networks. Malware can be used to steal personal information, carry out cyber attacks, and damage computer systems.

Cyberspace exploitation is a significant threat to national security, as malicious actors can use the internet to carry out cyber attacks on critical infrastructure, such as power grids, water treatment plants, and financial systems. These attacks can cause widespread harm, disrupt essential services, and pose a threat to national security. It is crucial for individuals and organizations to take steps to secure their computer systems and networks, and for governments to take steps to protect critical infrastructure. Only through education, awareness, and proactive security measures can we prevent the harm caused by cyberspace exploitation.

## **Infamous incidents of cyber terrorism**

Over a two-week period in 1998, ethnic Tamil guerrillas bombarded Sri Lankan embassies with 800 e-mails per day. "We are the Internet Black Tigers, and we're doing

This to disrupt your communications,"<sup>4</sup> the messages said. It was the first known terrorist attack on a country's computer systems, according to intelligence officials.

During the Kosovo conflict in 1999<sup>5</sup> hacktivists protesting NATO bombings targeted NATO computers with e-mail bombs and denial-of-service attacks. According to reports, businesses, public organisations, and academic institutions received highly politicised virus-laden e-mails from a variety of Eastern European countries. Web defacement was also prevalent.

The Electronic Disturbance Theater (EDT) has been conducting Web sit-ins against various sites in support of the Mexican Zapatistas since December 1997<sup>6</sup>. Thousands of protestors point their browsers to a target site at a predetermined time, using software that floods the target with rapid and repeated download requests. Animal rights organisations have also used EDT's software against organisations accused of animal cruelty. Another group of hacktivists, the electro hippies, staged Web sit-ins against the WTO when they met in Seattle in late 1999.

One of the most heinous cases of cyber terrorists at work occurred when crackers in Romania illegally gained access to the computers controlling the life support systems at an Antarctic research station, putting the 58 scientists on the line.

In May 2007, Estonia was subjected to a mass cyber attack by hackers inside the Russian Federation, which some evidence suggests was coordinated by the Russian government, though Russian officials deny any knowledge of this. This attack appears to have been in retaliation for the removal of a Russian World War II war memorial from downtown Estonia.

In January 2021, Hackers with ties to the Chinese government deployed ransomware attacks against five major gaming companies. They demanded over \$100 million in ransom.

---

<sup>4</sup> By BA Athulasiri Kumara Samarakoon, *The 3rd International Conference on Humanities and Social Sciences Ethnic Wars on Cyberspace: Case of Tamil Tigers and the Majoritarian Sinhalese State in Sri Lanka Proceedings-Culture and Defining of Meaning* (2011), [www.tamilnet.com](http://www.tamilnet.com), (last visited Feb 13, 2023).

<sup>5</sup> NATO - Topic: Kosovo Air Campaign (March-June 1999), [https://www.nato.int/cps/en/natohq/topics\\_49602.htm](https://www.nato.int/cps/en/natohq/topics_49602.htm) (last visited Feb 13, 2023).

<sup>6</sup> The Zapatista Movement: The Fight for Indigenous Rights in Mexico - Australian Institute of International Affairs

- Australian Institute of International Affairs,

<https://www.internationalaffairs.org.au/news-item/the-zapatista-movement-the-fight-for-indigenous-rights-in-mexico>

/ (last visited Feb 13, 2023).

In February 2021, Hackers tried to contaminate the water supply of Oldsmar, Fla., by exploiting a remote access system to increase the amount of sodium hydroxide present.

The Polish government said it suspected Russian hackers had taken control of Poland's National Atomic Energy Agency and Health Ministry websites for a short time in March 2021. They tried to spread alarms about a radioactive threat that didn't exist.

North Korea carried out a cyber attack against South Korea's state-run Korea Atomic Energy Research Institute by taking advantage of a virtual private network vulnerability in May 2021.

On May 30th 2021, cyber criminals breached the JBS network with ransomware, disrupting plants in the USA, Canada and Australia.

Iran used Facebook to target U.S. military personnel, posing as recruiters, journalists and nongovernmental organization personnel in July 2021. The hackers sent files with malware and used phishing sites to trick victims into providing sensitive credentials.

In September 2021, Hackers stole 15 terabytes of data from 8,000 organizations working with Voicenter, an Israeli company. The hackers offered the data online for \$1.5 million.

Brazilian hackers attacked a website belonging to Indonesia's State Cyber and Password Agency in October 2021.

Robinhood is a USA-based stock trading app. On November 3rd 2021, data of 7 million users was stolen and held to ransom by cyber criminals.

A Russian group claimed responsibility for a ransomware attack on CS Energy, an Australian utility company in December 2021.

On 23rd February, Nvidia, a major microchip producer suffered a data breach which saw source code fall into the hands of cyber criminals. The hacking group Lapsus\$ claimed responsibility for the attack, claiming it had stolen around 1TB of data.

One of the most widespread cyber breaches in history, WannaCry was a global ransomware attack that affected more than 200,000 computers in over 150 countries. WannaCry exploited a vulnerability in unpatched versions of the Windows operating system. This vulnerability was known as '**EternalBlue**', and had allegedly been developed in the US by the National Security Agency.

A national emergency was declared in Costa Rica in 2022 in the face of a series of ransomware attacks against critical institutions. An estimated 800 servers and several terabytes of information in the finance ministry were also impacted by the attacks.

### **Cyberterrorism v/s conventional attacks in cyberspace**

Cyberterrorism and conventional attacks in cyberspace are two distinct forms of malicious cyber activities that pose serious threats to organizations, businesses, governments, and individuals. Both forms of attack have significant impacts on their targets, but they have some differences in terms of their objectives, methods, and consequences.

Cyberterrorism is a form of terrorism that uses the internet, computer networks, and information technology to achieve political or ideological objectives. Cyberterrorists aim to cause fear, panic, and disruption through online attacks that can compromise sensitive information, disrupt critical infrastructure, or cause widespread panic. Cyberterrorists often use social engineering tactics to trick people into giving away their passwords, install malware on their devices, or compromise their personal information.

On the other hand, conventional attacks in cyberspace are malicious activities that target organizations and individuals with the primary goal of theft, destruction, or manipulation of data. These attacks are usually motivated by financial gain, competitive advantage, or personal grudges. Hackers, cybercriminals, and nation-state actors are among the most common perpetrators of conventional attacks in cyberspace. They use a variety of techniques such as phishing, malware, or advanced persistent threats (APTs) to compromise their targets.

### **Mitigation Initiatives for Cyberterrorism:**

#### **Convention on Cybercrime**

The Convention on Cybercrime, also known as the **Budapest Convention**, is the first international treaty aimed at addressing cybercrime and cyber security. It was adopted by the Council of Europe in 2001 and is the only binding international instrument that provides a comprehensive framework for the fight against cybercrime.

The Convention on Cybercrime establishes common standards for the investigation and prosecution of cybercrime and provides for international cooperation between states to address

these crimes. **It covers a wide range of offenses including computer-related fraud, child pornography, cyber terrorism, and unauthorized access to computer systems.** The Convention also provides for the protection of personal data and electronic privacy, as well as the criminalization of activities such as hacking, phishing, and other forms of cyber attacks.

### **Global Counter-Terrorism Strategy of the United Nations (UN):**

The United Nations (UN) has a crucial role in the global counter terrorism strategy, and it is committed to addressing the threat of terrorism through a comprehensive and coordinated approach with important pillars countering terrorism:

Measures to address the conditions conducive to the spread of terrorism, including poverty, conflict, and human rights violations.

Efforts to prevent and combat terrorism through the strengthening of national capacities and the development of international cooperation.

The protection of human rights and the rule of law, including the promotion of respect for human dignity, freedom, and equality.

### **UN Office for the Prevention of Terrorism (UNOPT):**

The United Nations Office for the Prevention of Terrorism (UNOPT) was established in 2017 as a dedicated office within the United Nations Secretariat to prevent and combat terrorism. The UNOPT is responsible for providing a comprehensive approach to preventing terrorism and its underlying drivers, including poverty, inequality, marginalization, and conflict.

The main objective of the UNOPT is to enhance the capacities of Member States to prevent terrorism and to promote cooperation and coordination among UN entities, Member States, and other stakeholders to prevent terrorism. This includes providing technical assistance and capacity-building support to Member States, supporting the implementation of relevant UN counterterrorism measures, and promoting international cooperation to prevent terrorism.

### **United Nations Security Council (UNSC):**

The United Nations Security Council (UNSC) is one of the six main organs of the United Nations and is responsible for maintaining international peace and security. The UNSC has a



significant role in addressing the threat of cyberterrorism, as it is the body responsible for the development and implementation of international security measures.

The purpose of the UNSC in addressing cyberterrorism is to ensure that cyberattacks do not escalate into a threat to international peace and security. The UNSC has adopted several resolutions on cyber security and cybercrime, including resolution 1373, which addresses terrorism in general, and resolution 1540, which focuses on the proliferation of weapons of mass destruction. The UNSC has also established a working group on cyber security and cybercrime to discuss and coordinate efforts to address these issues.

### **Counter-Terrorism Strategy of Brazil, Russia, India, China, and South Africa (BRICS):**

The Brazil, Russia, India, China, and South Africa (BRICS) group of countries have emerged as major players in global affairs, and their counter terrorism strategies play an important role in maintaining regional and international security.

In Brazil, the government has adopted a multi-faceted approach to countering terrorism that involves the development of strong laws and regulations, the strengthening of the country's intelligence and security services, and the promotion of international cooperation.

### **Shanghai Cooperation Organisation (SCO):**

The Shanghai Cooperation Organization (SCO) is a multinational political and economic organization founded in 2001. Its members include China, Russia, Kazakhstan, Kyrgyzstan, Uzbekistan, Tajikistan and India, with several observer states and dialogue partners.

The SCO has taken steps to address the threat of cyberterrorism and increase regional cooperation in the field of cybersecurity. The organization has recognized the increasing importance of the Internet and digital technologies in the modern world, and the potential for these technologies to be used for malicious purposes, such as cyberattacks and cybercrime.

The SCO has established a number of mechanisms to address cyber threats, including the creation of a Regional Anti-Terrorist Structure (RATS) to coordinate the fight against terrorism, extremism and separatism. Within RATS, there is a working group on information security that aims to enhance cooperation among member states in preventing and combating cybercrime and cyberterrorism

## United State of America

### Cybersecurity and Infrastructure Security Agency (CISA)

Cybersecurity refers to the practice of protecting computer systems, networks, and data from unauthorized access, theft, or damage. It involves implementing various technical, organizational, and physical measures to prevent, detect, and respond to cyber threats.

An estimated 53.35 million US citizens have been affected by cyber crime in the first half of 2022. Between July 2020 and June 2021, the US was the most targeted country for cyber attacks, accounting for 46% of attacks globally. US citizens lost \$6.9 billion in 2021 to cyber-related crimes, including romance scams (\$956 million), investment scams (\$1.4 billion) and business email compromise (\$2.39 billion).<sup>7</sup>

An Infrastructure Security Agency (ISA) is a government agency responsible for overseeing and managing the security of a country's critical infrastructure, such as its power grid, telecommunications networks, financial systems, and transportation networks. The ISA is responsible for implementing policies, standards, and guidelines to ensure the security of these critical infrastructure assets and to minimize the risk of cyber attacks, natural disasters, and other potential threats.

## ISRAEL

Israel is known for its advanced technology and innovative approach to cybersecurity, and its national cybersecurity strategy reflects this reputation. The 2017 National Cybersecurity Strategy of Israel is a comprehensive plan that outlines the country's approach to cybersecurity and the measures it will take to protect its critical infrastructure and citizens from cyber threats.

The strategy focuses on several key areas, including:

**Protecting Critical Infrastructure:** The strategy places a high priority on protecting Israel's critical infrastructure, including its energy, financial, and transportation networks, from cyber threats. This includes implementing stronger security measures and increasing the level of resilience and redundancy in these systems.

---

THE LATEST 2023 CYBER CRIME STATISTICS (February 2023)

<https://www.aag-it.com/the-latest-cyber-crime-statistics/> (last visited Feb 13, 2023).

**Cyber Defense:** The strategy calls for the development of advanced cyber defense capabilities to detect and respond to cyber-attacks, including the establishment of a national Cyber Defense Authority to coordinate the country's cybersecurity efforts.

**Cyber Intelligence:** Israel recognizes the importance of intelligence in the fight against cyber threats and calls for the development of a comprehensive national cyber intelligence capability.

**Cyber Education and Awareness:** The strategy also places a strong emphasis on cybersecurity education and awareness, both for the general public and for businesses, to help them better understand and address the risks posed by cyber threats.

**International Cooperation:** The strategy recognizes the importance of international cooperation in addressing global cyber threats and calls for increased cooperation with other countries and international organizations to enhance cybersecurity efforts.

### **United Kingdom (UK)**

The United Kingdom has a comprehensive national cybersecurity program that aims to protect its citizens, businesses, and critical national infrastructure from cyber threats. The program, which was established in 2009, is managed by the National Cyber Security Centre (NCSC), apart of the intelligence agency GCHQ. In 2022, 39% of UK businesses have experienced a cyber attack, the same as in 2021. However, this has dropped since 2020 (46%)

As of December 2022, 54% of UK businesses have acted to identify cyber security risks, up from 52% in 2021. However, the 2022 figures have dropped compared to 64% in 2020.<sup>8</sup>

The main objectives of the UK's cybersecurity national program are:

**Protecting Critical National Infrastructure:** The program places a high priority on the protection of critical national infrastructure, such as the energy, transportation, and financial sectors, from cyber attacks.

**Cyber Defense:** The NCSC leads the UK's efforts to detect and respond to cyber threats, working closely with government agencies, the private sector, and international partners to develop and implement robust cyber defense strategies

---

<sup>8</sup> THE LATEST 2023 CYBER CRIME STATISTICS (February 2023)

<https://www.aag-it.com/the-latest-cyber-crime-statistics/> (last visited Feb 15, 2023).

**Cyber Threat Intelligence:** The UK has a comprehensive cyber threat intelligence capability that provides real-time information on cyber threats to the government and private sector, allowing them to respond more effectively to these threats.

**Cybersecurity Awareness and Education:** The program also places a strong emphasis on cybersecurity awareness and education, providing guidance and training to individuals, businesses, and other organizations on how to better protect themselves from cyber threats. **International Cooperation:** The UK recognizes the importance of international cooperation in addressing global cyber threats and works closely with other countries and international organizations to enhance its cybersecurity efforts.

## **India**

Like many countries, India is suffering increasingly from cyber-crime. The number of cyber-related crimes reported in 2018 was 208,456. In the first 2 months of 2022 alone, there were 212,485 cyber-crimes, more than the entirety of 2018.

The figures rose more sharply through the pandemic, with reported crime jumping from 394,499 cases in 2019 to 1,158,208 in 2020 and 1,402,809 in 2021. Between Q1 and Q2 2022, cyber-crime across India increased by 15.3%.

Additionally, there have been an increasing number of Indian websites hacked in recent years. In 2018, some 17,560 sites were hacked. In 2020, an additional 26,121 sites were hacked. 78% of Indian organizations experienced a ransomware attack in 2021, with 80% of those attacks resulting in the encryption of data. In comparison, the average percentage of attacks was 66%, with the average encryption rate at 65%.

## **Information Technology Act: Cyber Terror Law**

The Information Technology Act of India,<sup>9</sup> enacted in 2000 and amended in 2008, is a legal framework that governs the use of information technology in India. The act is designed to provide a legal framework for e-commerce and to regulate the use of electronic records and digital signatures.

<sup>9</sup> The Information Technology Act, 2000, Acts of Parliament, 2000 (India).

The Information Technology Act of India contains provisions that relate to cyberterrorism and the use of information technology for illegal activities. For example, the act criminalizes unauthorized access to computer systems, the unauthorized interception of electronic communications, and the publication of false electronic information that causes harm to individuals or organizations. In addition to these provisions, the act also establishes the Office of the Cyber Appellate Tribunal, which has jurisdiction to hear appeals and disputes arising under the act.

National Cybersecurity Policy:

The National Cybersecurity Policy of India is a comprehensive policy framework that outlines the country's approach to cybersecurity and the measures it will take to protect its critical infrastructure and citizens from cyber threats. The policy was first issued in 2013 and has since been updated to reflect the evolving threat landscape and advancements in technology.

The policy focuses on several key areas, including:

**Critical Information Infrastructure Protection:** The policy places a high priority on the protection of critical information infrastructure, such as the energy, financial, and transportation networks, from cyber-attacks. This includes implementing stronger security measures and increasing the level of resilience and redundancy in these systems.

**Cyber Defense:** The policy calls for the development of advanced cyber defense capabilities to detect and respond to cyber-attacks, including the establishment of a National Cyber Coordination Centre to coordinate the country's cybersecurity efforts.

**Cybercrime Investigation and Prosecution:** The policy calls for the development of a comprehensive framework for investigating and prosecuting cybercrime, including the establishment of specialized cybercrime units within law enforcement agencies.

**Cybersecurity Awareness and Education:** The policy also places a strong emphasis on cybersecurity awareness and education, both for the general public and for businesses, to help them better understand and address the risks posed by cyber threats.

**International Cooperation:** The policy recognizes the importance of international cooperation in addressing global cyber threats and calls for increased cooperation with other countries and international organizations to enhance cybersecurity efforts.

## **Legislative reforms in india:**

India has made several legislative reforms aimed at improving cybersecurity and addressing the threat of cyberterrorism. Some of the major ones include:

**Information Technology Act, 2000:** This act provides a legal framework for electronic transactions and regulation of certifying authorities. It also lays down penalties for hacking, cyberstalking, and other cybercrimes.

**The Information Technology (Amendment) Act, 2008:** This amendment act expanded the definition of cybercrimes and increased the penalties for offenses such as cyber terrorism, identity theft, and cyberstalking.

**The Personal Data Protection Bill, 2019:** This bill aims to protect the privacy of individuals by regulating the collection, storage, and processing of personal data by companies. It also establishes a Data Protection Authority to enforce the provisions of the act.

**The Intermediary Guidelines and Digital Media Ethics Code, 2021:** This code lays down guidelines for online intermediaries, such as social media platforms and search engines, to regulate the publication of online content and to address issues such as cyberbullying, fake news, and disinformation.

**The Cryptocurrency and Regulation of Official Digital Currency Bill, 2021:** This bill aims to regulate cryptocurrencies in India and provide a framework for the issuance of an official digital currency.

## **Recommendations:**

In view of the expanding dimensions of computer-related crimes, there is a need for adopting appropriate regulatory legal measures and gearing up the law enforcement mechanism to tackle the problem of cybercrime with stern hands. A multi-pronged approach and concerted efforts of all the law enforcement functionaries is much more needed for effective handling of cybercrime cases. A common cybercrime regulatory law universally acceptable to all the countries would perhaps provide a viable solution to prevent and control cyber criminality.

## **Technological aspects:**

**Intrusion Management:** Process which primarily aims at precluding intrusions in the computer system therefore furnishing effective-security control medium.

**Self- regulation by computer and net druggies:** It's a process of developing a healthy law ofconduct by espousing a policy of restraint by both the computer druggies as well as the service providers.

**Use of voice-recognizer, sludge software and collar-ID for Protection:** Computers as a means for carrying out routine life conditioning, should be equipped with some safety andsecurity bias to cover against authorised operation of computer systems.

**Use of diligent Anti-Virus Softwares:** Antivirus software is a computer program which detects, prevents and takes action to protect the system and remove all malicious softwareprograms like viruses etc.

## **Legal Aspect:**

**Use of encryption technology:** To appoint well trained Information Security Officers who should be responsible for overall protection of computer coffers and for any lapse in computer security.

**Use of international treaties & agreements to present a combined front:** Ensures that all applicable local legislations are in harmony with international laws and conventions.

Establish progressive capacity building programmers for national law enforcementagencies.

## **Research Aspect:**

Improving awareness and competence in information security;

Develop foster and maintain national culture of cyber security;

To standardize and coordinate cybersecurity awareness and education programmes.

**Conclusion:**

In conclusion, cybersecurity and cyberterrorism are two important and interconnected issues that have significant impacts on the digital world. Cybersecurity focuses on protecting digital systems, data, and networks from unauthorized access, theft, and attacks, while cyberterrorism involves the use of technology to cause harm to individuals, organizations, or even governments. As technology continues to advance, the threat of cyberattacks and cyberterrorism will only continue to grow, making it crucial for individuals, organizations, and governments to take proactive measures to protect themselves from these risks. This can be achieved by staying informed about the latest cybersecurity threats, implementing strong security measures, and investing in the training and education of personnel. It's time for the Indian legal system to match its pace with the growing cyber crimes and the developing transnational justice around it as in the information age, openings to grow life for those who are stylish and suitable to use both technology and information. With the outpour of information to the cyber sphere with the arrival of COVID-19 epidemic the need for this change has become more imminent and necessary. Statutory laws, government programs, specialised probing agencies will go a long way in securing India's cyber spaces. The people ought to be equipped with enough knowledge to be suitable to defend themselves against the pitfalls of cyber crimes through legal mindfulness programmes. The unborn India's digital world lies on a fulcrum and the time to shift the fulcrum towards safety and security vis a vis cyber crimes is now.



## **DATA PROTECTION & ANTI-MONEY LAUNDERING – A COMPLEX RELATIONSHIP**

-Shubhangi Arde

### **Introduction**

With the rapid growth in the age of technology, everyone is open to surveillance and has lost their right to privacy from the government and all unknown agencies. In this no privacy era many unknown threats are coming at us at a faster rate. Right to Privacy is been defined in different aspects with the change in time. In the digital era we are facing privacy threats from unknown agencies situated at different corners of the world, where the right to privacy is been infringed in various aspects.

One of the upcoming threat waiting for us is the Anti- Money Laundering and Data Protection. Through this research paper the attempt is made to build a complex relationship between Data Protection and Anti-Money Laundering. Money Laundering Activities can be tracked down as far as thousand years back. Money Laundering is the method of illegally hiding the origin of money obtained from activities like gambling, corruption or drug-trafficking or any other activities where the source is unknown and utilizing that money by converting it in a legitimate way. It is an organized crime defined in different ways in different courses of the world.

In the earlier times the concept of money laundering was applicable only to the financial transactions for organized crime. Today, International organizations, multinational companies and fake institutions often expand it. In European Countries money laundering activities does not even need money transactions but any economic good. It is observed that money laundering is committed by private individuals, drug-dealers, businessmen, mafia members of criminal organizations or corrupt officials.

Hence in simple terms Money Laundering can be defined as the illegal process of making of large amount of money generated by criminal activity or converting black money into white money without paying taxes to the government. However this process is abused by some agencies to keep

money without any evidence of any criminal activities and to make use of it to supplement their annual budgets. Money laundering activities can be traced through several forms like Cash-Intensive business, Bulk- cash smuggling, Round- tripping, Gambling, open job market place such as freelancer.com.

- **Role of Financial Institutions in Anti-Money Laundering Activities.**

An effective Anti- Money Laundering programme needs a jurisdictions to crimes related to money laundering to make relevant regulators to give tools to and powers to police for investigations throughout the world to identify the source of money through financial institutions to report suspicious activities and risk based controls of their customers. To control money laundering activities strict background checks are required to strive against money launderers escape by through company structures and complex ownership.

Today, most of the financial institutions around the world and many non-financial institutions are required to report and identify transactions of suspicious nature to the intelligence bureau for instance, A bank verifies the customers identity through KYC, i.e. process of Know Your Customer, which means knowing the complete information of the customer and to tract financial background of the customer.

- **Privacy Concerns related to Anti-Money Laundering Activities**

Privacy means the capability of a person or a group of persons to hide information from others as well as to seclude themselves.<sup>29</sup>The Right to Privacy is recognized internationally as Human Rights under Article 12 of the UDHR<sup>30</sup> which provides everyone has the right to not to get disturbed or interfered with his privacy, family, correspondence or his personal information. Indian

---

<sup>29</sup>Dr. Payal Jain & Ms. KanikaArora, “Invasion of Adhar on right to privacy; Hugh concern of issues & challenges 45(2) Indian ILR 33-35(2018).

<sup>30</sup>Universal Declaration of Human Rights

Judiciary and many jurists have spread ink to define Right to Privacy and its limitations. After Independence many cases were filed before Indian courts for the protection of Right to Privacy.

In recent times with the digitalization, the infringements of right to privacy concerns are increasing at an alarming rate. Our current Prime Minister Shri Narendra Modi has seen a dream of Digital India and have launched the same in 2016. Since then almost everyone is moving forward towards digital world. No doubt that Digital India campaigns is a big success for the last 7 years life has become easier. Everything is available at one touch. But at the same time it lacks in the protection laws and leaking the personal data of people and inviting unknown agencies through world.

In 2016 after demonetization, all the citizens were asked and promoted to shift to online banking and insisted to link the Bank accounts with financial tools like Gpay, Paytm, Phonepay, Amazon Money, Whatsapp Money and so on. While all these facilities were very convenient and time saving for consumers but by linking the bank accounts and accepting terms and conditions with Institutions is more risky without any legislation.

Anti- Money Laundering activities and Data Protection have a complex relationship, as all the facilities are available at our tip of the mobile phone, the personal information of the personal is also available to all those agencies worldwide. Hence we all are at a very high risk of unknown threats. To convert the black money into white money has become easy for these agencies as they have a good number of data available with them. Therefore it is high time to have data protection legislation in India like all the European countries, The Data Protection Bill is pending in the parliament for last five years. All the government, non-government financial institutions are awaiting for this Bill, as many of these activities would be restricted.

One of the Major concerns for anti money laundering and data protection is funding of the terrorist activities. The main problem is to know the source of money to criminals where they do not rely on one specific financial institution for their financial needs; criminals usually diversify multiple institutions and jurisdictions across world. And the use of fake corporate vehicles is extensive as

it provides criminals the anonymous identity they need. Worldwide efforts have taken the corporate veil of privacy in some jurisdictions via introducing laws requiring greater transparency of corporate controller and Ultimate Beneficial Owners (UBOs). This conflict of privacy versus information sharing with terrorist and criminals played out in private information-sharing threats.

### **Data Privacy breach and its associated risk**

The state processes personal data for multiple of purposes, and is arguably its largest processor. In India, the state uses personal data for purposes such as the targeted delivery of social welfare benefits, effective planning and implementation of government schemes, counter-terrorism operations, etc. Such collection and use of data is usually backed by law, though in the context of counter-terrorism and intelligence gathering, it appears not to be the case. Across India, both central and state government institutions are launching platforms to digitize records and offer online services to citizens. Establishing such platforms is leading to a more comprehensive digital trail on individuals. Government initiative such as parivahan sewa, Digi Locker, Aadhar, IRCTS, Bharat Interface for Money (BHIM), TARKASH by Ahmedabad city Police . Personal data is quite valuable and will continue to be collected, stored and processed on a large scale in India. While technology and business models using personal data have evolved significantly, the regulations and ethics around data usage and privacy are still evolving in India.<sup>92</sup>

Personal data is used by big markets to support personalized services. The government uses it to provide various public services in an efficient manner. The data scientists do the task of designing and developing new protocols and algorithms. Users get benefit via personalized consumer experiences. Data are turning to be the pillar of the big market.

The terms information and data are both used in the context of informational privacy and data protection. The word has specific connotations in the fields of computer science and information technology. Information on the other hand simply means facts about something or someone. Under Section 2(1) (v) of the IT Act information includes data, text, images, sound, voice, codes, computer programmes, software and databases or micro-film or computer generated micro-fiche.

Big Data is usually characterized by Vs, namely volume as in massive datasets, velocity which relates to real time data, and variety which relates to different sources of data. Other technological developments such as artificial intelligence, machine learning, the Internet of Things are all part

of the Big Data ecosystem and their use is becoming increasingly common place While Big Data does not have a precise definition it can be understood as essentially involving gathering large quantities of data and applying innovative technology such as predictive analysis to them to extract knowledge.

The biggest challenge in regulating emerging technologies such as Big Data, artificial intelligence and the Internet of Things, lies in the fact that they may operate outside the framework of traditional privacy principles. Big Data involves the processing of large data sets, usually the source of such data may not be directly from the individual, and consent may not be as relevant. Further, data may be generated as a by-product of a transaction or obtained by a service provider in return for a free service such as free email accounts, social networks etc. or obtained as a consequence of accessing a service such as use of GPS navigation, and it may not be possible to specify the purpose for which personal data is collected at the time of collection. The advent of such technologies has also expanded the very definition of personal data.

Hence Personal Data Protection is the need of an hour, as personal data has become the new business strategy of the market. In the last few years worldwide concepts of richest man of the world has changed. Bill Clinton was said to be the richest person in the world, depending upon his assets and bank balance but in today's world the Elon Musk is known to be the richest man of the world as he possess the maximum data of the world. Population is always treated as the asset of the country but then personal data of the people without their consent is said to be negative asset of any of these organizations.

Privacy no doubt implies protection of personal rights liberty and thus if it is disturbed it should have been with reasons. With the development of telecommunications, internet, e-governance, e-commerce and rapid growth in the software right to the personal data protection is much needed. Although information and telecommunication technologies have enhanced the capacities to collect, process store and communication information, it is these very capacities of technology which makes us weak to intrusions of our privacy.

Further our personal data available on our personal devises like Computers, Mobile Phone, Social media accounts could compromise us in unpleasant ways- the consequences like Financial loss, online stalking, or using our personal details for illegal activities. Moreover in the age of cloud

computing when our personal data like our chats, call logs, bank accounts, personal profiles our online communications is available on distant servers of the worldwide multinational companies makes it difficult to trace the source of culprit behind the infringement of personal data.

Although there are technological measures through which these unwanted risks could be reduced, it is also important to have a strong legislation in place which lays emphasis on protection of personal data and privacy. Besides the urgent need of protection of personal data, improper attention to data protection practices and economic cost to implement anti money laundering laws, may cost to individuals privacy rights. In June 2011, the data protection advisory committee to the European Union issues a report on data protection issues related to the prevention of money laundering and terrorist financing, which identified numerous transgressions against the established legal framework on privacy and data protection. The report made recommendations on how to deal with money laundering and terrorist sponsorship in ways that protects personal privacy rights and data protection laws. In the United States, groups such as the American Civil Liberties Union have expressed concern that money laundering rules require banks to report on their own customers, essentially conscripting private businesses "into agents of the surveillance state"

Many countries are obligated by various international instruments and standards, such as the 1988 United Nations Convention Against Illicit traffic in Narcotic Drugs and Psychotropic Substances, the 2000 Convention against Transnational Organized Crime, the 2003 United Nations Convention against Corruption, and the recommendations of the 1989 Financial Action Task Force on Money Laundering (FATF) to enact and enforce money laundering laws in an effort to stop narcotics trafficking, international organized crime, and corruption. Mexico, which has faced a significant increase in violent crime, established anti-money laundering controls in 2013 to curb the underlying crime issue.

## **SCOMET- EXPORT CONTROL AND WHY IS IMPERATIVE FOR INDIA**

- *Joshua Ebenezer.*

### **Need for a robust strategic control system**

A major threat to civil society is the spread of artilleries weapons of destruction ("WMDs") and their means of delivery. The widespread dissemination of WMDs raises the possibility that Governments may use them (as seen by the Iran/Iraq conflict) and that terrorist organisations and non-state actors will acquire them and use them in acts intended to cause extensive death and destruction.

According to reports, 19 countries now produce cruise missiles, and roughly 75 countries currently own them<sup>31</sup>. The launch industry is seeing an increase in the number of nations and commercial organisations, which is also changing the security picture in space.

The fact that more and more states are building proliferation capability presents a further obstacle. International anxiety over North Korea's nuclear and missile programmes has been significant. With regard to chemical non-proliferation, the risk of using chemical weapons against civilians was demonstrated during the Syrian conflict.

Given the ease of access to information and the complexity involved in producing biological weapons, there is a real concern that proliferators will create new strains of harmful viruses. While supporting the creation of novel medical treatments, recent synthetic biology research also raises the possibility of the emergence of brand-new infections. The ability of the authorities to comprehend and recognise potential dangers is now more difficult.

<sup>31</sup> Feickert A. Cruise Missile Proliferation <https://fas.org/sgp/crs/nuke/RS21252.pdf> & McCarthy W.J. Directed Energy and Fleet Defence Implications for Naval Warfare

As the "Fourth Dimension" of warfare, cybersecurity has become a crucial security factor. Particularly, there are chances that these products contain built-in capabilities for dual use and could be abused against vital aspects of infra or stealing IP like trade secrets, in businesses.

More importantly, since more and more elements are incrementally increasing in trafficking through unlawful procurement plans and employing sophisticated-advanced methods to escape controls, the risks of WMD proliferation are no longer restricted to states (e.g., using a procurement network of a host of syndicates and methods to hide the end-use, by moving restrictive goods as well as sensitive goods via transshipment hubs or local institutions).

#### Transformations in global economic activity

Increasing international trade and the connected data network boost countries' ability to obtain dual use technologies, in an illegitimate and legitimate way impacting along integrated value chains, proliferation hazards spread across national boundaries and legal systems as proliferators exploit their complexity and susceptibility.

Due to global supply chains, there is also an increase in the quantum of dual-use items are being transhipped through other countries, (3<sup>rd</sup> parties) raising the possibility that these goods will be diverted to problematic nations. Additionally, online trade platforms are changing the structure of supply chains as exports are more frequently "transmitted, not moved." Anyone, anyone can participate in a dual-use export transaction as a middleman or broker thanks to these platforms.

Given this difficult circumstance, a strong strategic control mechanism is essential to preventing the spread of these products for the sake of international security.

India's efforts in this area aren't just focused on becoming a trustworthy country with a strong export control system; they're also intended to help the country acquire access to better technology and materials for its civilian programmes, such fuel for atomic power plants. But a strong Export Control system is a requirement in order to guarantee the free flow of technology. A robust Export Control regime is a *sine qua non*.

### **India's international commitments**



Before we go into the legal framework in India, we shall see India's International commitments in this regard.

#### A) Formal Membership

- **The International Atomic Energy Agency ("IAEA"): 1971**

- IAEA aims to encourage nuclear energy peaceful use while discouraging facilitating any military goals, including the development of nuclear weapons. India is an IAEA founding member.

- **Biological Weapons Convention: 1972**

- The Biological Weapons Convention, sometimes known as the "BWC," is an international multilateral treaty that prohibits the production, development and stock-piling of biological (bacteriological) and weapons of toxins as their destruction. Since 1974, India participated in the BWC. India is committed to preventing the creation, manufacture, and storage of chemical and biological weapons as a signatory to this pact.

- **Chemical Weapons Convention ("CWC"): 1993**

- The CWC is a pact on arms control that forbids the development, acquisition, and application of chemical weapons and their precursors. The CWC is being implemented by the Organization for the Prohibition of Chemical Weapons (OPCW), an intergovernmental agency. Since 1996, India has participated in this convention.
- To satisfy the OPCW deadline, India voluntarily destroyed its entire stockpile of chemical weapons on March 16, 2009

- **Missile Technology Control Regime: 1987**

- The G7 developed nations formed the multilateral export restriction framework known as the MTCR in April 1987. (Canada, France, Germany, Italy, Japan, the United Kingdom, and the United States of America).
- India submitted a formal membership application to the organisation in June 2015, and on June 27, 2016, it was accepted with the active support of France and the United States.

- **The Hague Code of Conduct (Ballistic Missiles): 2002**

- The ICOC, also known as The Hague Code of Conduct ("HCOC"), was added to the MTCR in 2002. The HCOC is the outcome of efforts made on a global scale to control access to ballistic missiles that have the capability of delivering WMD. India joined the HCOC as a signatory on June 1, 2016.

#### B) Voluntary Membership

- **Wassenaar Arrangement: 1996**

- The Wassenaar Arrangement is an Export Control for Conventional Weapons and Dual-Use Products & Technology, sometimes known as the Wassenaar Arrangement ("WA"), is a MECR with 42 participant states. It was established on July 12, 1996, in Wassenaar, the Netherlands.
- On December 7, 2017, India became the 42nd member state. India has managed to join the Wassenaar group despite not being a signatory to the NPT on nuclear weapons, which would strengthen its credentials in the non-proliferation arena.

- **Australia Group (Chemical & Biological): 1985**

- The Australia Group (the "AG") is an informal group of nations that works to prevent exports from advancing the development of chemical or biological weapons by harmonising export regulations.
- India became a member of the MTCR and Wassenaar on January 19, 2018, and as a result, it joined the AG.

#### **India and the Nuclear Supplies Group**

The Nuclear Suppliers Group (NSG) is a multilateral export control system and a consortium of nuclear-supplier nations that aims to stop nuclear proliferation by limiting the export of goods that can be used to make nuclear weapons.

India is not a member of the NSG because of the present rules, which specify that no country can join if it has not ratified the NPT.

India has two nuclear explosions under its belt: in 1974 and 1998. India was one of the few nations with a no-first-use policy, which forbade the use of nuclear weapons unless an enemy had already attacked with them. India's nuclear programme is openly known, and

China appears to be preventing India from joining the NSG despite not having to sign the NPT.

### Why are export controls relevant for India?

India has to have a have a robust export control system to-

- India must have a reliable export control system to prove that it is a trustworthy exporting country.
- ensuring that other countries selling to India are making reciprocal steps to regulate their exports, and that the transfer of cutting-edge technology in vital fields is possible. For instance, the US's designation of India as having the Strategic Trade Authorization-1 status ensures that India is qualified to receive transfers of cutting-edge defence equipment. Indian status was upgraded as a result of India's enhanced export control procedures and adherence to international export control regimes, according to US Commerce Secretary Wilbur Ross.<sup>32</sup>
- meet the requirements to join the elite Nuclear Suppliers Group ("NSG"): India is making every effort to meet the requirements for membership despite strong opposition from China

### India's commitments under Other Multilateral agreements

In this regard, India joined multilateral agreements like the Nuclear Non-Proliferation Treaty (NPT) and Chemical Weapons Convention (CWC), as well as other multilateral export control regimes (MECR) like the Wassenaar Arrangement (WA), the Nuclear Suppliers Group (NSG), the Australia Group (AG), and the Missile Technology Control Regime (MTCR).

### **India's export control regime -SCOMET**

Special Chemicals Organisms Materials Equipment and Technology is known as SCOMET in India. The term "SCOMET" refers to a collection of goods, equipment, and technologies that have the potential to be used in WMDs or military applications.

<sup>32</sup> Source: US Department of Commerce website <https://www.commerce.gov/news/press-releases/2018/07/us-secretary-commerce-wilbur-ross-announces-programs-increase-us>

The Hague Code of Conduct (HCOC), Wassenaar Arrangement, Australia Group (AG), Chemical Weapons Convention (CWC), Biological Weapons Convention (BOC), Missile Technology Control Regime (MTCR), Hague Code of Conduct (HCOC), and UN Security Council Resolution (UNSCR) 1540:2004 are just a few of the multilateral treaties that India has agreed to.

Except for Category 7, whose items are included in Category 8, SCOMET is a self-contained list with eight distinct categories and precise definitions for inclusions and exclusions. The list was last updated on December 30, 2022, and is currently in effect.

Hence, SCOMET is essentially another tool in the arsenal of the Indian enforcement agencies for export controls. The fact that the controls cover not only the equipment but also the technology employed in each of these fields and the software created or used for these reasons is more significant. Hence, service exports will be a subject that the Indian enforcement authorities have not previously focused on in terms of export control and would be scrutinised by these agencies for compliance.

### **Catch-all controls:**

The Wassenaar Arrangement's inclusion of India led to the introduction of this all-encompassing control clause. Yet, compared to the all-encompassing controls suggested by the Wassenaar Arrangement, the provision chosen by India is substantially stricter.

Wassenaar's all-encompassing controls were intended to prevent the transfer of non-listed dual use items to nations under a binding United Nations Security Council arms embargo or any relevant regional arms embargo that a Participating State is either required to abide by or has voluntarily agreed to comply with. without any mention of a target, in their missile system or military end use (even by terrorists and non-state actors).

But the catch-all controls imposed as a consequence to this requirement by India, is actually an across-the-board restriction for all dual use items that the exporter, *'knows or has reason to believe'* have a potential risk of use in or diversion to WMD or in their missile system or military end use (including by terrorists and non-state actors), without any reference to any destination.

## Legal framework in india

### India's fight against proliferation

India has been actively bolstering its export control systems and working to align them with several MECRs, including the MTCR, CWC, and the Hague Code of Conduct and International Code of Conduct Against Ballistic Proliferation.

The following statutory measures, in the author's well-considered judgement, are sufficient at this time to demonstrate India's commitment to a strong controlling export control regime:

- *Foreign Trade (Development and Regulation) Act, 1992* (“FTDR Act”); Foreign Trade Policy (“FTP”) and the Handbook of Procedures (“HBP”)
- Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005
- The *Atomic Energy Act, 1962*
- The *Customs Act, 1962*
- Rules for the Manufacture, Use, Import, Export and Storage of Hazardous Microorganisms/Genetically Engineered Organisms or Cells, 1989

### Dual use - A potential mine-field

For the unwary exporters, the prescription for the dual use items and the all-encompassing restrictions create a potential minefield. For instance, a substance as harmless as triethanolamine, which is a pH balancer in many cosmetic preparations and is classified as a Category-1 Hazardous Chemical (IC017) and so subject to export restrictions, is a precursor to chemical weapons.

The PlayStation 2 was seen as dual-use technology due to its capacity to produce high-quality photographs quickly—a characteristic shared with missile guiding systems.

Chemical weapons can also utilise chlorine, a substance that is present in many everyday things (such as bleaching powder). A wide range of products also uses electronic chips.

Semiconductors, for example, are essential parts of numerous devices, including computers, cars, wind turbines, solar panels, etc. These semiconductors are also used in military equipment, such as missile directing systems and night vision cameras.

The emergence of cutting-edge, state-of-the-art tech with double-use applications, such as cloud computing, nanotechnology, manufacturing/3-D printing additives, or research of graphene, is increasing the difficulty of strategic controls. The difficulty presented by technology transfers is growing as a result of additive manufacturing. Legal actions are being taken in the US because export control laws from 2013 forbade the "publishing" of a 3-D printed firearm.<sup>33</sup>

India is experiencing growth. India will consequently need to strike a difficult balance between concerns about proliferation on the one hand and the industry's legitimate economic interests on the other.

Evidently, India has been actively constructing a strong export control system that, at least on paper, will compete with any advanced export control system, such as that of the United States or the European Union. So, India has reason to be proud of its advancements in this field, even though much more work needs to be done in terms of implementation. A seat in NSG would not be as far fetched as it seems if the effort is consistent with the rhetoric. To accomplish this, though, India will need to tightrope walk quite a bit.

<sup>33</sup>Defense Distributed v. United States Department of State, 838 F.3d 45

## **Legality of Prostitution in India - A Jurisprudential aspect with regards to safeguarding and rehabilitation of sex workers.**

Dr. Keval Govardhan Ukey

Associate Professor, School of Law, Sandip University, Nashik

Email: [kevalukey@rediffmail.com](mailto:kevalukey@rediffmail.com)

Mr. Amar Suresh Salve

Ph.D.(Law) Research Scholar, School of Law, Sandip University, Nashik Email:

[amarslv@gmail.com](mailto:amarslv@gmail.com)

### **Abstract:**

Prostitution is not new to our society; it is as old as civilization itself. It is deep rooted in our society and has been a part of Indian society ever since the idea of marriage came into existence. In the current scenario, prostitution entangled with the draconic problems of devastating violence, inequitable discrimination and exploitation. Prostitution is often considered as a taboo in Indian society, and somewhere requisite attention has not been paid for its regulation. This paper examines the nexus between the increasing criminality against sex workers and the growing need to legalize and regulate prostitution in India. The main focus is in providing legal safety and the process of rehabilitation of this deprived section of the society. There have been various statutes enacted in this regard by the post and pre – independence governments regarding prostitution, and also a number of books and articles on its legalization. In spite of the fact that in different cases the Hon'ble Supreme Court of India has communicated the view that this calling ought to be legalized in India. Today our country's biggest concern is a massive increase in the number of incidents of assault and legalizing prostitution would be one step forward towards fighting assault. This paper analyzes the broad aspect of problems arising due to criminality in the prostitution and to combat these problems using law as an effective instrument by legalization of prostitution in India.

Keywords- Prostitution, legalization, rehabilitation, sex workers, criminality.

Introduction:

Prostitution is the exchange of sex for money, with those involved referred to as prostitutes. Its legality and regulation vary worldwide. Prostitution is part of the sex industry, with brothels being dedicated establishments for it. Opinions on prostitution differ globally, with some seeing it as exploitation while others see it as a valid occupation. In past Indian society, prostitutes were called 'Devadasi' and dedicated themselves to Lord Krishna. Devadasis believed they were wedded to gods and couldn't marry humans. They're also known as 'Nagarvadhu' or 'town brides.' Royals and rich folks employed them to perform. Devadasis were respected before British rule but when British officers arrived in India and watched their performances, it led to one-night stands. British officers solicited artists for sex, sparking prostitution in India and reducing temple dances. During British rule, Indian women sold themselves to British people for money as the economy worsened. Japanese women were also brought to India as sex slaves under Portuguese rule. During Company Rule in India, brothels were established by the military, using village women and girls who were paid directly. Poverty and unemployment are some of the reasons women engage in prostitution. Women in remote areas are often exploited by intermediaries promising job opportunities, but then sell them into prostitution due to poverty.<sup>1</sup> Poverty often leads to prostitution. 6% of women turn to prostitution after rape, while many survivors face shame and stigma. Society blames rape victims and families reject them, causing further harm and delay of justice. Girls who can't find shelter or hope in society often turn to prostitution. 8% of them have experienced incest, mainly with their father or uncle. "Victims of incest forced into prostitution due to lack of safety, along with other contributing factors."

### **Literature Review:**

In his 2016 article, Md Rahaman discusses human trafficking in South Asia, focusing on Bangladesh, India, and Nepal. Poverty, illiteracy, and globalization are identified as contributing factors. The main aim of human trafficking is to exploit victims through forced labor, debt bondage, child labor, and sex work.<sup>2</sup> Prostitution debate ruled by 2 feminist groups: radical and liberal. Radicals claim it supports male dominance, driven by poverty leading to exploitation. Their argument is that a prostitute's consent is irrelevant if violence and exploitation are present since it contradicts the principle that one cannot consent to having their rights violated.

---

<sup>1</sup> Ratnamala and Another v. Respondent AIR 1962 Madras 31.

<sup>2</sup> Md Rahaman (2015) "Human Trafficking in South Asia (Special Preferences on Bangladesh, India and Nepal): A Human Rights Perspective" IOS



Prostitution is often pursued by women with few options and is marked by violence. Prostitution attracts trafficking, making it a form of slavery. However, liberal feminist groups argue that women have the right to choose and their decision to engage in prostitution should be respected. Prostitution critics believe banning it makes exploitation worse. Old-fashioned views on sex are rooted in patriarchy. Liberal feminists say prostitution is consensual if paid, while non-consensual activity is wrong. Observe prostitution within the context of societal practices influenced by existing laws and misogyny. JG Raymond's 2004 article in *Violence against Women* explores the legal debate surrounding prostitution since the mid-1980s.<sup>3</sup> Netherlands and Germany legalized prostitution, including pimps, brothels and buyers. Thailand prohibits prostitution but tolerates brothels and sex tourism.

Sweden penalizes buyers but decriminalizes prostituted women.

**Objectives:**

1. To identify the various challenges that female prostitutes face due to policy framework and inadequate implementation of existing laws.
2. To investigate the extent to which the Right to Life and Right to Profession, as guaranteed by the Constitution of India to all citizens, are applicable to female prostitutes for their upliftment and improvement of living conditions.
3. To analyze the role of government bodies and NGOs in rehabilitating female prostitutes and their children, promoting their overall development.
4. To examine the role of the Indian judiciary in protecting the rights of female prostitutes and their children, while also providing timely guidance to the government to take necessary steps in this regard.
5. To critically evaluate various international instruments that provide for the rights of female prostitutes across the globe, which helps in understanding the international legal framework available for them.

---

<sup>3</sup> Janice C. Raymond (2004) "Prostitution on Demand: Legalizing Buyers as Sexual Consumers", *Violence against women* 10(10) 1156

6. Based on the findings of this study, recommendations will be made to improve the sociolegal status of female prostitutes and provide appropriate rehabilitation for their children.

**Hypothesis:**

1. The Constitution of India grants fundamental rights to all citizens, including female prostitutes. However, these rights, particularly the Right to Life, Personal Liberty, and the Right to Profession, are often denied to them, leading to their exploitation and vulnerability to abuse.
2. Female prostitutes face exploitation in various ways, which also affects the future of their children, who are often ostracized from society and forced into the same profession. This lack of education and opportunity deprives them of pursuing other careers.
3. The existing legal system is insufficient in protecting the rights of female prostitutes and their children. While prostitution is illegal, the laws do not address the need to protect the profession of women who turn to it for survival.
4. Proper policy framework for regulating prostitution and providing rehabilitation for the children of female prostitutes could lead to opportunities for them to explore new professions and lead a better life. Governmental and non-governmental bodies have an essential role to play in rehabilitating female prostitutes and their children, enabling them to become responsible citizens of the country.

**Research Methodology:**

This research aims to explore regularization and rehabilitation in female prostitution laws and their impact on children of prostitutes, using a mix of empirical and non-empirical survey methods. This study aims to explore the regulation of female prostitution and rehabilitation programs for their children. Both quantitative and qualitative data will be collected to understand the research components. The study is significant due to the challenges faced by female prostitutes, which impact their living conditions and survival. The government does not protect female prostitutes despite constitutional rights and Indian Judiciary guidelines. The judiciary's role is vital in achieving the welfare state's goals. Analyzing laws meant to protect female prostitutes but finds they hinder their profession. We must decide whether to embrace or ignore prostitution. Legalizing prostitution has benefits such as reducing child prostitution, empowering sex workers to report

violations, improving health with safe sex, generating taxes, reducing trafficking and minors in prostitution, reducing rape cases, and giving sex workers client choice. Age requirements for female prostitutes would also prevent health damage and continuing careers as they age. Legalizing prostitution benefits sex workers by empowering them to report violations of their rights and enabling safer sex practices. This would end sex workers' bribes and enable them to pay taxes like other professions, while licensing would decrease trafficking and minors' involvement. Legalizing prostitution reduces rape instances and gives sex workers client choice.

**Judicial Aspect:**

India's Immoral Traffic Act of 1956 defines prostitution as commercial sexual exploitation or abuse. Mumbai alone has 100,000 sex workers, contributing to Asia's largest sex industry with approximately 10 million sex workers across India. 20,000 women and children were sex trafficking victims in India in 2016. Sex workers lack legal protection, face stigma, marginalization, and numerous forms of abuse. Sex workers lack human, health, and labor rights and struggle for equality. COVID-19 has hit them hard as they can't work without clients and can't find new jobs easily.<sup>4</sup> The 1956 Immoral Traffic (Prevention) Act is inadequate to manage the Indian sex industry and provide aid to sex workers and trafficking victims. Prohibiting brothels, solicitation, and public proximity prostitution has not decreased prostitution. The Act increased sex workers' vulnerability and limited their access to healthcare. Sex workers are denied access to public facilities, hindering their chances of improving their lives. Mainstreaming sex work, providing birth control and medical aid, and education can prevent their exploitation. Addressing motivations for voluntary sex work and punishing sex traffickers, while rehabilitating forced sex workers is vital. However, IPC laws on prostitution are limited. The ITPA restricts prostitution and penalizes related acts, as outlined in the following sections.

---

<sup>4</sup> The Immoral Traffic (Prevention) Act, 1956 [indiankanoon.org](http://indiankanoon.org)

- Section 3 pertains to the punishment for keeping a brothel or allowing premises to be used as a brothel. The term "brothel" is defined in section 2(a) of the Act as any house, room, or place used for prostitution.<sup>5</sup>
- Section 4 penalizes any person who is living off the earnings of prostitution, including family members.<sup>6</sup>
- Section 5 targets pimps, brothel owners, and traffickers by penalizing the act of procuring, inducing, or taking a person for prostitution.<sup>7</sup>
- Section 6 targets middlemen and brothel owners who detain sex workers in brothels or other premises where prostitution takes place.<sup>8</sup>
- Section 7 penalizes prostitution carried out in public places or their vicinity, including densely populated areas, hostels, religious places, educational institutions, hospitals, nursing homes, and other places notified by the Commissioner of Police, Magistrate, or state government. The vicinity is defined as two hundred meters.<sup>9</sup>
- Section 8 penalizes sex workers for seducing or soliciting a person for the purpose of prostitution. This section is discriminatory, as it prescribes different punishment for men and women for the same offense, with men receiving half the punishment prescribed for women.<sup>10</sup>

### **Civic Initiatives:**

Prajwala is an organization established by Sunitha Krishnan in 1996 with the objective of preventing inter-generational prostitution. The NGO aims to assist the victims of sex trafficking and sex crimes by rescuing and rehabilitating them. They also provide support to rape victims through their Rape Victim Support Programme (RVSP) and protect witnesses through the Victim Witness Protection. Prajwala works on five pillars: Prevention, Protection, Rescue,

---

<sup>5</sup> Ibid

<sup>6</sup> Ibid

<sup>7</sup> Ibid

<sup>8</sup> Ibid

<sup>9</sup> Ibid

<sup>10</sup> Ibid

Rehabilitation, and Reintegration. It has become a prominent advocate for women and children worldwide.<sup>11</sup>

Guriya, founded in 1993 by Ajeet Singh, fights human trafficking and forced prostitution, with a special focus on child prostitution. It also works to eliminate hunger and poverty, which are the leading causes of such crimes. Guriya's plan of action includes filing Public Interest Litigations (PILs) to support their rescue operations, and so far, they have filed 15 PILs and booked 77,000 cases against perpetrators. They have rescued over 2,500 girls from a red-light area in Varanasi. International Justice Mission (IJM) collaborates with the Central and state governments to combat bonded labor and sex trafficking. They rescue victims of trafficking who have been sexually exploited for commercial purposes and provide rehabilitation assistance to survivors. The organization also brings perpetrators to justice and has secured justice for at least 132 survivors. IJM works with grassroots-level NGOs and community-based organizations to empower vulnerable members through their various awareness programs on human trafficking and related legal procedures.

**Conclusion:**

Neo-abolitionists argue that prostitution reinforces male dominance and is driven by poverty, leading to exploitation of women, their children, and their future. This study aims to explore the regularization of laws on female prostitution and rehabilitating children of prostitutes. Despite guidelines from the Indian Judiciary and constitutional rights for female prostitutes, the government has yet to take protective measures. The researcher explores laws meant to protect female prostitutes' rights, but instead hindering their profession. Legalizing prostitution has numerous advantages, including reducing child prostitution, empowering sex workers to report abuses, enhancing overall health, increasing revenue through taxes, hampering trafficking and minors' involvement, lowering rape cases, and giving sex workers the freedom to choose their clients. They rescue trafficked individuals who were sexually exploited for profit and assist in their rehabilitation.

---

<sup>11</sup> Vaishali singh (2017) "Legalising prostitution in India" Probono India Publication 2017

**Bibliography:**

- [1] D. R. Kailash, *Constitutional Law of India*, Allahabad: Central Law Publication, 2001.
- [2] B. D.D., *Introduction to the Constitution of India*, New Delhi: Wadhwa and Company Law Publishers, 2002.
- [3] B. P. M., *The Constitution of India*, Delhi: Universal Law Publishing Co., 2006.
- [4] S. R. Narayan, "Prostitution: A Brief History," 12 2 2018. [Online]. Available: <https://www.speakingtree.in/allslides/prostitution-a-brief-history/child-prostitution-in-india>.
- [5] "The Immoral Traffic (Prevention) Act, 1956," [Online]. Available: [www. indiankanoon.org](http://www.indiankanoon.org).
- [6] J. C. Raymond, "Prostitution on Demand: Legalizing Buyers as Sexual Consumers," *Violence against women*, p. 10 (10) 1156.
- [7] M. Rahaman, *Human Trafficking in South Asia (Special Prefences on Bangladesh, India and Nepal): A Human Rights Perspective*, IOS, p. IOS.
- [8] A. Mathieson, E. Branam and A. and Noble, "Prostitution Policy: Legalization, Decriminalization and Nordic Model," *Seattle Journal for Social Justice*, vol. 14, no. 2, 2016.
- [9] "Memorandum on Reform of Laws Related to Prostituin in India," Center for Feminist Legal Research, 1999.