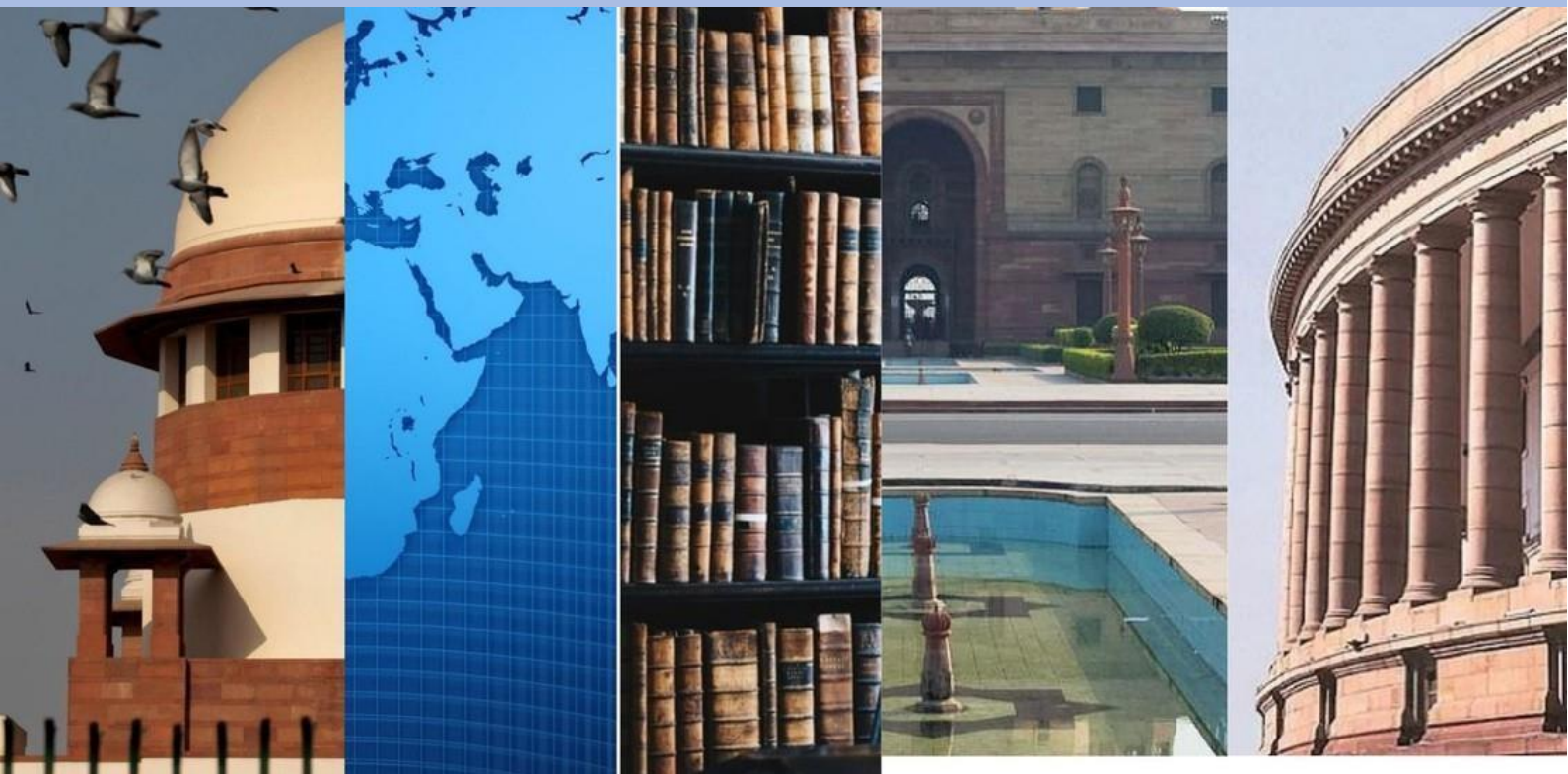


# **Journal of Global Research & Analysis**

**A Multi-Disciplinary Peer-Reviewed Research Journal**  
**RNI-HARENG/2012/59126** **ISSN: 2278-6775**



**Volume 14(1)**

**JUNE 2025**

# **Journal of Global Research & Analysis**

[A Bi-Annual (June & December)]

**Multi-Disciplinary Peer-Reviewed Research Journal]**

**editorjgra@geetalawcollege.in**

**RNI-HARENG/2012/59126**

**ISSN: 2278-6775**

## **PATRON IN CHIEF**

**MR. S.P. BANSAL**  
CHANCELLOR, GEETA UNIVERSITY PANIPAT, HARYANA

## **PATRONS**

**MR. NISHANT BANSAL**

PRO-CHANCELLOR,  
GEETA UNIVERSITY,  
PANIPAT, HARYANA

**MR. ANKUSH BANSAL**

PRO-CHANCELLOR,  
GEETA UNIVERSITY  
PANIPAT, HARYANA

## **EDITORIAL BOARD**

**EDITOR-IN-CHIEF**

**DR. SUBHASH KUMAR**

PROFESSOR & PRINCIPAL  
GEETA INSTITUTE OF LAW, PANIPAT

## **EDITORIAL BOARD MEMBERS**

**DR. PRERNA DAWAR**

PROFESSOR & DIRECTOR (TRAINING)  
GEETA INSTITUTE OF LAW, PANIPAT

**DR. SANDEEP SAINI**

ASSOCIATE PROFESSOR & HOD  
GEETA INSTITUTE OF LAW, PANIPAT

**DR. VIKAS NANDAL**

ASSISTANT PROFESSOR (SOCIOLOGY)  
GEETA INSTITUTE OF LAW, PANIPAT

**MS. CHINKY NANDA**

ASSISTANT PROFESSOR (LAW)  
GEETA INSTITUTE OF LAW, PANIPAT

**MS. DHRITI**

ASSISTANT PROFESSOR (LAW)  
GEETA INSTITUTE OF LAW, PANIPAT

## **PEER REVIEW PANEL**

---

***Prof. (Dr.) Richa***

*Director, School of Law, Maharaja Agrasen University, Baddi, Himachal Pradesh*

***Dr. Kuldeep Chand***

*Professor of Law, School of Law, Maharaja Agrasen University, Baddi, Himachal Pradesh*

***Dr. Krati Rajoria***

*Associate Professor of Law, National Law Institute University, Bhopal*

***Dr. Kusum Pal***

*HOD & Associate Professor, Amity Law School, Amity University, Mohali, Punjab*

***Dr. Cholaraja Mudimannan***

*Assistant Professor, Campus Law Centre, University of Delhi, New Delhi*

***Dr. Geetika Sood***

*Assistant Professor, Department of Laws, Himachal Pradesh University, Shimla*

**Journal Website:**

## **OWNED BY**

---

**K.R Education Society, 547, Sector-11 (HUDA), Panipat, Haryana**

**All rights reserved. No part of the contents may be reproduced in any form without the written permission of the publisher. Journal of Global Research & Analysis is an open forum that encourages critical research engagement. However, views expressed in its pages are the contributor's own and do not represent the opinions or policies of the Journal of Global Research & Analysis.**

**Published by Nishant Bansal** (On Behalf of) K.R. Education Society, Panipat.

**Address of Publisher** – H.No. 547, Sector -11 (HUDA), Panipat, Haryana, **Owned by** K.R. Education Society, 547, Sector 11 (HUDA), Panipat, Haryana, **Editor** – Dr. Subhash Kumar, **Place of Publication**– K.R. Education Society, 547, Sector -11 (HUDA), Panipat, Haryana, India.

## **DISCLAIMER**

---

### **JOURNAL OF GLOBAL RESEARCH AND ANALYSIS**

Journal of Global Research & Analysis (JGRA) is “**A Bi-Annual Multi-Disciplinary Peer-Reviewed Research Journal**” (Print) in English for the enhancement of research published by Geeta Institute of Law (GIL) under the aegis of K. R. Education Society, Panipat.

Geeta Institute of Law (GIL) under the K. R. Education Society, Panipat, shall be the sole copyright owner of all the materials published in the Journal. Apart from fair dealing for the purposes of research, private study, or criticism, no part of this Journal can be copied, adapted, abridged, translated, or stored in any retrieval systems, computer systems, or other systems or be reproduced in any form by any means whether electronic, mechanical, digital, optical, photographic or otherwise without prior written permission from the Society.

The editors, publishers, and printers do not own any responsibility for the views expressed by the contributors and for the errors, if any, in the information contained in the Journal and the author shall be solely responsible for the same.

## ARTICLES

---

### 1. Cyber Bullying and Privacy Breaches

*Avni and Dr. Subhash Kumar* ..... 1

### 2. E-commerce data breaches: liability of online platforms under consumer protection law

*Sombir Gulia* ..... 12

### 3. DNA profiling and privacy in India: A critical appraisal of the 2019 DNA regulation bill and new criminal laws with comparative perspectives from the USA, UK and EU

*Tannu Gupta and Vinod Kumar* ..... 23

### 4. Juvenile trials: improving legal, social and mental health in juvenile justice

*Vijay Kumar Verma and Priyanka Bhati* ..... 42

### 5. Virtual harassment but real harm-a study on sexual offences against women in digital environment and need for legal reforms in India

*Veena Nirudhiya* ..... 54

### 6. Corporate social responsibility (CSR) and its impact on corporate governance

*Samay Jain* ..... 67

### 7. "Faking Reality, Real Consequences: Regulating Deepfakes and Sextortion in the Digital Age"

*Divya Girsu and Preet Deswal* ..... 85

### 8. Navigating the digital childhood: reimagining consent, guardianship, and autonomy in India's data protection regime for children

*Suji Cheriyana* ..... 101

### 9. India's juvenile justice system; bridging the gap between legislative intent and implementation reality

*Shalini Shukla* ..... 110

<b>10. The Telecom Act, 2023: a future – ready framework or a constitutional regression</b>	
<i>Charupragya Ksuhwaha</i> .....	127
<b>11. A Critical evaluation of the Competition (Amendment) Act, 2023</b>	
<i>Dr. Isha Wadhwa Sharma</i> .....	137
<b>12. Empowering Clean Energy: Legal Pathways to Renewable Energy Adoption in India</b>	
<i>Snigdha Sharma and Nikhil Sharma</i> .....	160

## **CYBER BULLYING AND PRIVACY BREACHES**

AVNI\*

DR. SUBHASH KUMAR\*\*

---

### **ABSTRACT**

The internet and the technologies make life faster and easier, but they also bring new and serious problems. The internet brings challenges such as cyberbullying, privacy breaches, fake news, online fraud, addiction, the digital divide, job loss from automation, and rising cybercrimes like hacking and scams. Cyberbullying and privacy breaches are two major issues. Cyberbullying means using mobile phones, computers, or social media to insult, threaten, or embarrass someone. Privacy breaches mean someone's private information is stolen, shared, or used without permission. This study discusses impacts of these crimes on public, importance or needs to resolve. Further this study covers studies and suggestions given by many experts and scholars. In India we have laws like the Information Technology Act, 2000, and the Hon'ble Supreme Court of India recognizes "privacy as a fundamental right"; these steps show the importance and need of protections. At international level we have the "General Data Protection Regulation" (GDPR); it also provides safety and further directs to amend the laws with new technology like artificial intelligence, deepfakes, and smart devices. To resolve these issues, we need to come together with the solutions, like- Governments, schools, parents, digital companies, and society must all work together. If we discuss it further, it is very important to provide necessary requirements for the victims, like safe online behaviour, strong digital education, secure platforms, and mental health support, etc. We need global cooperation and constant research, by which the digital world can remain safe, respectful, and useful for everyone; otherwise, it will be difficult to handle such issues.

**Keywords:** Cyberbullying, privacy breaches, digital literacy, legal frameworks, online safety, data protection, mental health

---

\* LLM Student, Chandigarh university, Mohali, Punjab  
\*\* Professor & Principal Geeta Institute of Law, Panipat

## **1.INTRODUCTION**

In this present time internet make a good importance without using internet, a single day it is very important because all the tasks are done by the help of internet, most of the offices govern through internet. Our life becomes habitual of it, it has slowly become a space where most of our daily activities take place like- people study online, run businesses, meet friends, share personal thoughts, and even seek entertainment through digital platforms<sup>1</sup>. While this change has made life easier in many ways, it has also created some serious risks and issues which need to be resolved. Two major issues or problems faced by internet users, are cyber bullying and privacy breaches. These two issues are affecting each and every one, not limited to one age group or one country—they cut across boundaries and affect people everywhere. Cyber bullying is simply bullying that takes place through technology<sup>2</sup>. It may involve insulting messages, spreading lies, sharing embarrassing photos, or even threatening someone over the internet. What makes it more harmful than traditional bullying is that it does not stop once the victim leaves school or work<sup>3</sup>. The bullying continues on phones, computers, and social media platforms, making it hard for people to find relief. A single post or video can be shared thousands of times, damaging reputations in minutes or in seconds. Many young people, in particular, find it overwhelming because the online world is deeply tied to their social lives. Due to this, victims are suffering from stress, anxiety, and in some cases, long-lasting trauma. For examples continuous harassment has led to extreme steps like- self-harm or suicide cases<sup>4</sup>. Privacy breaches, on the other hand, highlight a different danger of the digital age. Whenever people use websites, apps, or online services, they leave behind personal information—names, photos, contact numbers, bank details, or even simple browsing habits. This information can easily be misused by the hackers or cyber frauds. Sometimes hackers steal it, while at other times, even companies themselves use it without proper consent<sup>5</sup>. The result is that people lose control over their own data. For some persons, it may bring financial losses and for others, it is the feeling of being exposed or unsafe that troubles them most. Unlike cyber bullying, which is visible, privacy violations often happen silently, and victims realize the impact only after the damage has been done to him.

---

<sup>1</sup> Pew Research Center, "The Internet and Daily Life," 11 August 2004,

<sup>2</sup> StopBullying.gov, "What Is Cyberbullying?" last modified August 11, 2004,

<sup>3</sup> Sameer Hinduja & Justin W. Patchin, *Cyberbullying: An Overview of the Research* (Cyberbullying Research Center, 2025)

<sup>4</sup> Jessica Ortega-Barón et al., "Joint Association of Bullying and Cyberbullying in Health-Related Quality of Life in a Sample of Adolescents," *International Journal of Environmental Research and Public Health*, vol. 16, no. 24, 2019,

<sup>5</sup> Anjali Sharma, *Cyberbullying and Its Impact on Mental Health: A Study of Indian Adolescents* (Ph.D. Thesis, University of Delhi, 2023)

Taken together, cyber bullying and privacy breaches show that technology is a double-edged sword. It can connect, but it can also harm<sup>6</sup>. It is pertinent to mention here, that it is very important to resolve these issues and need strong awareness, education, strict/adequate and appropriate laws, and responsible behaviour from all stakeholders<sup>7</sup>. People need to understand that safety and respect should apply to the online world in the same way they apply in real life. To prevent the benefits of the technology we need to take further to resolve such issues, otherwise it may become a big problem in future<sup>8</sup>.

## **2.DEFINITIONS**

It is necessary to describe cyber bullying and privacy breaches precisely before trying to comprehend them. Both are closely related to the digital era, but the behaviors that lead to them—harassment, intimidation, and invasion of privacy—have been around for a long time.

**2.1 Cyber Bullying:** The Cambridge English Dictionary says that cyber bullying is "the use of electronic communication to bully someone, usually by sending them messages that are threatening or scary<sup>9</sup>." The Oxford Advanced Learner's Dictionary also says that it is "the act of using computers, mobile phones, or other devices to upset or hurt someone on the internet<sup>10</sup>." Both descriptions stress two main ideas: the use of technology and the desire to hurt or scare someone. Cyberbullying is different from regular bullying because it may happen anywhere and at any time. It typically leaves a lasting digital record.

**2.2 Breaches of Privacy:** Privacy breaches happen when someone gets into or uses personal information without permission. According to the Cambridge Dictionary, a privacy breach is "a situation in which someone's private information is accessed, shared, or used without their permission<sup>11</sup>." The Oxford English Dictionary defines it as "the act of disclosing or misusing personal or sensitive information without consent<sup>12</sup>." In today's world, this includes hacking, stealing someone's identity, releasing personal photos without permission, or companies or other people using private data in ways that aren't allowed.

---

<sup>6</sup> TSS Rao, "Cyberbullying: A Virtual Offense with Real Consequences," *Journal of Family Medicine and Primary Care*, vol. 7, no. 3, 2018

<sup>7</sup> Colin Murphy, *Cyberbullying among Young People: Laws and Policies in Selected Member States* (European Parliamentary Research Service, 2024)

<sup>8</sup> BP Hendry, "Recommendations for Cyberbullying Prevention and Education," *Journal of School Health*, vol. 93, no. 4, 2023,

<sup>9</sup> Cambridge English Dictionary, "Cyberbullying," *Cambridge University Press*,

<sup>10</sup> Oxford Advanced Learner's Dictionary, "Cyberbullying," Oxford University Press,

<sup>11</sup> Cambridge English Dictionary, "Data Breach," Cambridge University Press,

<sup>12</sup> Oxford Learner's Dictionaries, "Data Breach," Oxford University Press,

### 3. LITERATURE REVIEW

Cyberbullying and privacy breaches are closely related issues in the online world; harmful actions often rely on the theft or misuse of personal information, and when privacy is compromised, it exacerbates the harm and complicates finding solutions. Study goes into law, social things, and tech—from rule and policy to the study of young people, how platforms work, and the idea of privacy. A good answer needs a clear law, platform duty, teaching digital people, and making tech that keeps privacy safe. The six writers show strong and useful work in this area: lawmen, research people, and thinkers whose writing changes policy, schoolwork, and ideas of privacy in social media time.

#### **3.1 Author name: Sameer Hinduja, book name: *Bullying Beyond the Schoolyard*, title: *Preventing and Responding to Cyberbullying***

Sameer Hinduja's work looks at numbers, effects, and stopping cyberbullying in young people. With Justin Patchin, Hinduja makes school and community plans, lessons, and rules for answers. Their study mixes survey, case story, and policy talk to show risk (like hiding names and platform ways), victim effect (mental health and study harm), and protection (parent watch and school mood). For privacy breaks, they show how sharing personal detail, forcing image sharing, and doxxing make harm bigger and make it harder to heal—so they say we need to learn privacy and law in anti-bullying plans. Their work is used by school and policy people as a clear guide for cutting online harm and still keeping young people's privacy and freedom<sup>13</sup>.

#### **3.2 Author name: Justin W. Patchin, book name: *Bullying Beyond the Schoolyard*, title: *Preventing and Responding to Cyberbullying***

Justin Patchin gives a part with Hinduja: Patchin focuses on changing the study to real school rules, police training, and parent guides. He shows simple tools—report ways, proof keeping, and talking with the platform—to help victims of cyberbullying and privacy breaches get answers. Patchin also shows the tech side of privacy harm (image sharing, group chat, and place leaks) that makes more attacks. His work (class, policy note) helps normal people know how to write down a case in law, use the right way, ask the platform to remove it, and work with the school to keep the child's privacy right. Patching, pushing on clear steps, and putting all sides together are key to making law work in real-life cases<sup>14</sup>.

---

<sup>13</sup> Sameer Hinduja and Justin W. Patchin, *Bullying Beyond the Schoolyard: Preventing and Responding to Cyberbullying* (Sage Publications, latest edition).

<sup>14</sup> Justin W. Patchin and Sameer Hinduja, *Bullying Beyond the Schoolyard: Preventing and Responding to Cyberbullying*

**3.3 Author name: Danah Boyd, book name: It's Complicated, title: The Social Lives of Networked Teens**

Danah Boyd gives a detailed story study on how teens use online places—and what rules and privacy ways they use. Not like people say teens are careless; Boyd shows careful acts: teens make privacy by rule, by choosing who sees, and by picking platforms. This show matters for cyberbullying because it shows how normal privacy acts (like sharing in a friend circle) can break when sharing goes wrong and how social things (status, leaving out) push online hurt. Boyd says policy must see teen growth needs, and the platform must make designs that support context privacy (so data in one place is not used badly in another). Her work joins social study and design for safe teen online life<sup>15</sup>.

**3.4 Author name: Daniel J. Solove, book name: Understanding Privacy, title: Understanding Privacy (Harvard Univ. Press)**

Daniel Solove's work on the idea shows privacy is not one single right but many kinds of problems. For cyberbullying and privacy breaks, his list (like data take, data join, name show, and data share) helps to see how acts like doxxing or image sending break different privacy and cause much harm. The solve idea also helps the law look at different answers (stop order, money payment, privacy case, and data rule) that fit different harm types. His easy map is used by lawmen and rule makers who build privacy laws that also stop personal data use from hurting online<sup>16</sup>.

**3.5 Author name: Helen Nissenbaum, book name: Privacy in Context, title: Privacy in Context: Technology, Policy, and the Integrity of Social Life**

Helen Nissenbaum's theory of context integrity says privacy hopes come from rules of information flow in place. In cyberbullying, her idea shows why sharing in a friend group is okay, but the same sharing goes wrong when it moves places (private to public) or breaks norms (like a personal photo put to shame). This is big for policy and platform rules: the answer must see if the info move breaks the context norm and if the platform makes it easy or hard to misuse. Her theory helps design that which keeps privacy (stops easy sharing and sets group control), and the law sees detail by context, not one same rule for all.<sup>17</sup>

---

(Sage Publications, latest edition).

<sup>15</sup> Danah boyd, *It's Complicated: The Social Lives of Networked Teens* (Yale University Press, 2014).

<sup>16</sup> Daniel J. Solove, *Understanding Privacy* (Harvard University Press, 2008).

<sup>17</sup> Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford University Press, 2010).

## **4. HISTORICAL EVOLUTION**

Cyber bullying and privacy breaches are new words, but the actions they describe—harassment, humiliation, and violation of privacy—have been around for a long time. You may see how they changed throughout time by looking at the ancient, mediaeval, pre-digital contemporary, and digital eras.

### **4.1 Ancient Period (Before 500 CE)**

In ancient cultures, people mostly spoke to one other instead of writing things down or sending handwritten notes. Forms of bullying and privacy abuses occurred even before contemporary technologies. Public mocking and humiliation were frequent ways to impose social standards in ancient Greece and Rome (800 BCE–500 CE). People may be embarrassed in public areas like markets and assemblies, and false allegations could damage a person's image for good. The Roman practice of "damnatio memoriae," which removed a person's name and pictures from public records, is an early example of targeted defamation that is similar to internet abuse today. The Manusmriti and other books from ancient India (about 500 BCE to 500 CE) talk about using social shame to change behavior. This shows that societies have used humiliation to enforce regulations in the past. Even though contemporary privacy didn't exist, people regarded political and personal secrecy very highly, and violations of private information were treated very severely<sup>18</sup>.

### **4.2 Medieval Period (500 CE – 1500 CE)**

In the Middle Ages, letters, messengers, and printed papers made it easier to talk to each other. This gave people new tools to harass or invade private. Both the church and the state punished slander and defamation in mediaeval Europe. People might occasionally utilize public announcements, pamphlets, and town criers to damage people's reputations. In mediaeval Islamic countries and India, anyone may read couriers' communications for political or personal gain, which was an early infringement of privacy. Public humiliation was still common. People who broke the law may be shamed in public places, which is like modern-day cyberbullying. During this time, people started to realize how vital privacy was. Nobility wanted private ways to send letters, plan military operations, and trade. More and more, people thought that interfering without permission was wrong or against the law<sup>19</sup>.

### **4.3 Pre-Digital Modern Period (1500 CE – 1970 CE)**

---

<sup>18</sup> Amit Kumar, "Cyberbullying and Cyberstalking Laws in India," *African Journal of Biomedical Research* 27, no. 2 (2024): 1–10,

<sup>19</sup> Christian Lange, "Privacy in Islamic Law", *Oxford International Encyclopedia of Legal History* (Oxford: Oxford University Press, 2009)

The printing press, followed by the telegraph and telephone, made communication faster, but it also made it easier for people to harass and invade privacy. Like current cyberbullying, newspapers and pamphlets often have false information that hurt people's reputations. People worried about eavesdropping and getting into communications without permission when telegraphs and phones were invented. These were seen as both moral and legal wrongs. Privacy was recognized by the law for the first time in the late 1800s. In their 1890 essay for the *Harvard Law Review*, Samuel Warren and Louis Brandeis spoke about the "right to privacy," which means being safe from unwelcome exposure<sup>20</sup>.

#### **4.4 Digital Period (1970 CE – Present)**

The arrivals of computer, mobile technologies and software make it more complex, it changed the way people talk to each other. The digital platforms which are using, it made abuse faster, more widespread, and more anonymous, while also making privacy violations bigger<sup>21</sup>.

**4.4.1 Cyber Bullying in the Digital Age:** By using digital resources, like- Online gaming, social media, and messaging applications are all new places where people might be harassed and suffered these types of issues because the messages, pictures, and videos may go across the globe in a matter of minutes, and they frequently leave indelible marks. This leads to persistent harassment and mental trauma. People who faced or suffered may feel anxious, depressed, and very upset. This is impacting teenagers at first stage because this generation “can stay without food not without phone or internet” this becomes a significant problem<sup>22</sup>.

**4.4.2 Privacy Breaches in the Digital Age:** While using the technology every time we leave a digital trail. Hackers, identify thieves and businesses use this information for political or commercial gain. The Cambridge Analytica scandal (2018) and other high-profile incidents showed that millions of people's personal data were used without their permission, showing how big privacy breaches are these days. Privacy violations, on the other hand, don't always happen loudly, and victims only realize how bad things are after a lot of harm has been done.

---

<sup>20</sup> Samuel D. Warren & Louis D. Brandeis, “The Right to Privacy,” *Harvard Law Review*, Vol. 4, No. 5 (15 December 1890), pp. 193-220.

<sup>21</sup> Lee Rainie, Sara Kiesler, Ruogu Kang & Mary Madden, *Anonymity, Privacy, and Security Online*, Pew Research Center Report, 5 September 2013.

<sup>22</sup> Chanda Maurya, T. Muhammad, Preeti Dhillon & Priya Maurya, “The effects of cyberbullying victimization on depression and suicidal ideation among adolescents and young adults: a three-year cohort study from India,” *BMC Psychiatry*, Vol. 22, Article 599 (2022).

## **5. ANALYSIS AND DISCUSSION**

Cyberbullying and privacy problems grow with technology but still show old human behavior like public shaming or reading private messages. Cyberbullying, helped by anonymity and the internet everywhere, hurts the mind, social life, and daily routine, while privacy breaking harms self-respect, dignity, and trust. Laws like India's IT Act and world law like GDPR give some protection, but law use and tech follow are slow. To prevent it, we need education, technology safety, and social support because the new technology like- AI and deepfakes makes more risk which needs active watching, honest design, and online learning to reduce harm and prevent individual rights of the individuals.

**5.1 Understanding Cyberbullying:** Cyberbullying is the similar as the normal bullying but it committed by using technology and online sources. This type crime can be committed anytime, anywhere, and is often hidden. Mostly threatening messages, sharing private photos without permission, fake accounts, and false rumors spread fast and leave a permanent online trace which harm or effects victims for a lot of time. Though its online, effect is real on mind as well as to social life, and routine of the victim. Old times also have the same behavior—public shame, mockery, intercepted letters—showing human acts are the same; only the tools change. Research by Hinduja and Patchin shows cyberbullying is not only for young adults; adults also face harassment at work or in social places. In India, Duggal shows a rise in online harassment as social media grow. Online hidden identity helps bad people, and victims feel helpless. Now cyberbullying is a worldwide problem; we need a new way to stop and prevent harm.

**5.2 Psychological and Social Impacts:** Its effect is very serious; it is not just a short upset because it effects the victims for a long time. Because of this, victim feel anxiety and depression, they stay away from people, and their self-respect falls in the eyes of themselves as well in the eyes of the society. In serious cases, harassment may leads or convert it to suicidal thoughts or suicidal cases. Socially, victims avoid online and offline life, increase loneliness, and break community bonds. Families are also confused and don't know how to help. Privacy breaks add more problems. Unauthorized access, identity theft, or big data leaks reduce trust of persons, organizations, and governments. Worldwide, the mental and social effect is high; counselling and digital learning are needed.

**5.3 Legal and Policy Measures:** To reduce such type of cases we need strong laws which may provide justice to the victims. In India, the IT Act 2000 and the Supreme Court case Puttaswamy v. Union of India (2017) give some protection. But law use is slow, and law does not match fast tech, say Duggal and Gupta. World laws like the EU GDPR give strict rules for data and focus on consent, transparency, and responsibility. Still, problems remain in real time and across the country. In India law mainly

focuses on awareness and legal reform, we do not have such appropriate law which may reduce such type of crimes. International law focuses on following rules, ethics, and system protection, but we need to understand law alone is not enough we need education, technology, active watching and required regular amendments as per the needs.

**5.4 Technology, Challenges, and Prevention:** Technology can help to reduce such type of crimes because these are committed by the use of technology only. It becomes a challenge because by using technology social media, messaging apps, and online games can spread bad content fast; and due the weak security makes it worse. AI can find bad language but fail in context, sarcasm, and culture, so a human check is needed. To stop this problem, we need mix of tech, education, and social plans. School, work, and online communities teach safe online acts. Security like encryption, two-step login, and content checks reduce privacy risk. We need to provide counseling sessions, friends support, and community programs which may reduce stress and help victims. Experts say education must fit culture; world studies show best practices like AI transparency, live monitoring, and world teamwork. Best stop when social, tech, and law work together.

**5.5 Emerging Trends and Future Outlook:** AI content can be used to harass; deepfakes can harm with fake videos or photos. Digital records are now permanent, with more long-term risk for the person and organization. Future plans must focus on active monitoring, world teamwork, and honest tech design. Honest AI, live content checks, and strict laws reduce harm. We need to provide education because it can provide knowledge people, “to spot and stop online threats”. A mix of national awareness and world best practice gives strong protection. History shows tech changes, but the human behaviour behind bullying and privacy breaks remains the same. The solution must fix social and tech problems to work well.

## **6. CONCLUSION**

Cyberbullying and privacy breaches problems are very big issues in today’s world of the internet. These problems are not only related to technology problems; they are also, human mind problems like-shame, hurt feelings, and breaking personal limits. Now, the internet makes problems faster and bigger as compare to the prior time where we do not have such facilities. Now, messages, photos, and videos go viral or easily circulated everywhere very fast, it gives long-time pain and social trouble to the victims. Privacy breaking also hurts, disrespect, breach trust of a person. In this ongoing time, it becomes very difficult to identify the “data misuse” because many times it is hidden by the hackers or offenders. To fix these problems, we need a strong plan, while implementing the adequate and appropriate laws, which ensures justice shall be served to the victims and individual rights and privacy

may be protected. National law as well as the international law both shall be strong then only, we can deal this matter, because this is very serious and very important to catch the guilty, protect people, and stop crime. New laws or policies shall provide with the provisions which cover new technology like AI, deepfakes, and other digital tools. That shall provide with clear punishment and ways to act across countries. It further very important to understand this issue, we need to provide appropriate training or teaching to children, parents, and teachers about online safety and required majors shall be taken like-reduce fear of reporting, it may reduce crime. It shall also be inserted under the new policies/laws that mental help and social support are also very important, like counselling, friends support, and a safe place for people to recover from bullying or data problems. Technology is helpful as well as it becomes a danger, because the lack of strong actions against the offenders.

To reduce such crimes, it is very important that world-wide collaborations may be performed as a teamwork because cyber risks go across countries, and it need cooperation, good technology, and sharing the best way are needed for safe internet. Technology will change life, but law, school, family, and internet companies must work together. Law, education, technology, and social help together can make the internet safe without hurting the respect, privacy, and safety of a person.

## **7.SUGGESTIONS AND RECOMMENDATIONS**

To stop cyberbullying and privacy problems, strong legal protection is very important. There must be special laws for online harassment, identity theft, and data misuse, with clear punishment and ways to act across countries. Teaching people about internet safety in school, work, and community is also very important to make them careful and reduce fear of reporting. Technology must be used with strong security, AI checking, and clear data rules. For recovery, victims basically need mental help and counselling sessions.

**7.1 Strengthening Legal Protections:** One important step to fight with cyber bullying and privacy problems is to make law stronger. In India, Information Technology Act, 2000 and Supreme Court's Puttaswamy v. Union of India (2017) judgment giving privacy as fundamental right, gives base, but fast growth of technology makes gaps in law use. Need special law for online harassment, identity theft, revenge pornography, and misuse of personal data. Law also must have clear punishment, fast courts, and way to act across countries because cybercrime go beyond national boundary. European Union's GDPR law is a good example for clear rules, responsibility, and consent in data use. India and other country can follow same rule to make organizations act right and protect personal information. Law must be checked and updated again and again to face new problems and new technology.

**7.2 Promoting Digital Literacy and Awareness:** Education is a very strong tool which can stop cyberbullying and privacy problems. Schools, colleges, and workplaces must give training and digital learning programs to teach safe online behavior, how to protect privacy, and how to face such matters. Young people must be trained to know bad content and report it safely. Parents and guardians must also guide children to use the internet safely. Awareness programs on social media, TV, and in the community can reduce fear of reporting and make victims ask for help. By teaching people about the risk and result of online action, society can make a habit of responsibility and care in the digital world.

**7.3 Leveraging Technology for Prevention:** Technology needs to be trained, by which itself can help stop cyberbullying and protect privacy. Internet platforms must use strong security like- encryption, two-step login, and live monitoring. AI tools should analyse, find bad content or suspicious activity shall be blocked/prohibited. To increase the awareness, we need to make organizations and committees which may tell, about how should we collect, keep, and share data so users can control their personal information from the hackers. Regular security checks, timely updates, and honest system design shall be adopted which may decrease the risk of breaches and make people trust digital platforms more.

**7.4 Mental Health and Social Support:** It is important to understand the impact it has on emotional and social health of the victims, like anxiety, depression, and staying away from people it may cause or increase the victims towards the suicidal thoughts. Further to resolve this issue, victims need strong counselling, friends support programs, and community help to handle stress and recover from pain. Schools and workplaces can make safe places to report problems, talk about feelings, and get advice. Families should have some knowledge to deal with victims accordingly to increase or provide victims well and happiness, like- open talk, support, and quick action can stop more mental harm and give victims strength to act against bullying also a support to deal in this situation.

**7.5 Research, Monitoring, and Global Collaboration:** As new technologies are coming day by day, like- AI, deepfakes, and the Internet of Things, the way and size of cyber threats are also changing and it is increasing accordingly. To handle or resolve this type of issues it is important to continuous research, watching, and data study to know the trends and make plans as per the needs. Government, school, and private companies must work together to share knowledge, make rules, and follow the best way. Global cooperation is also critical because digital platforms operate internationally. Ethical design, real-time monitoring, and coordinated policies can address cross-border threats effectively.

## **E-COMMERCE DATA BREACHES: LIABILITY OF ONLINE PLATFORMS UNDER CONSUMER PROTECTION LAW**

Sombir Gulia\*

---

### **ABSTRACT**

The fast growth of e-commerce in India has changed the way people buy goods and services. It gives convenience and easy access and saves time. But with this growth comes big risks to consumer data privacy and safety. E-commerce platforms collect and store a lot of personal, financial and transaction information which may be used by hackers and data breaches. The theft of consumer data can result in financial loss, identity theft, reputational damage, and decreased trust in online shopping. This creates legal and ethical problems for platforms and shows the need for clear rules about their responsibility under consumer protection law. In India, the Consumer Protection Act, 2019 and the Information Technology Act, 2000 deal with such matters, protect consumers' rights, including privacy, safety and protection from unfair practices. Section 2(1)(o) defines "unfair trade practices," which includes poor data security, and Sections 2(1)(r) and 2(1)(d) cover privacy and protection. Hon'ble Apex Court of India made it clear that platforms cannot avoid responsibility by saying they are only intermediaries. Judicial decisions suggested that platforms must have a strong security, inform users quickly if breaches happen and also fix the problem properly as earlier as possible. Even with these laws, problems continue. While deciding who is responsible or accountable it becomes hard when platforms, sellers, payment gateways or cloud providers handle such data. Cross-border transactions and fast-changing technology make it more difficult. Other countries having legal framework like: the EU is having GDPR, the USA is having CCPA and Singapore is having a strict rule about data protection. These legal frameworks include strong security, mandatory reporting of breaches and giving certain rights to their consumers. This research looks at India's legal system for e-commerce data breaches. It studies the history, court decisions, and responsibilities of online platforms under consumer protection law. It points out gaps in laws, challenges in enforcement, and the role of regulators. Protecting consumer data is not only a legal duty but also important for business, because losing trust can hurt growth. Based on this, the paper suggests steps to make online commerce safer. These include clear rules for platform liability, standard security guidelines, mandatory breach notifications, stronger regulatory checks, teaching consumers about their rights, and learning from

---

\* LLB Student, Chandigarh university, Mohali, Punjab

international best practices. These steps aim to make e-commerce safer, build trust, and make platforms accountable while helping the market grow.

**Keywords:** E-commerce, Data Breach, Consumer Protection Law, Online Platforms, Liability, Privacy, Information Technology Act, Consumer Rights

## 1. INTRODUCTION

E-commerce is growing very fast in the twenty-first century. It changes how people buy things, use services, and do online payments. In day today life digital services, e-commerce websites and apps like Amazon, Flipkart and Paytm Mall are now part of life without these our life very will be difficult. In India, on digital platforms we have lot of users. The growth of users is increasing day by day and it is good because it gives easy access, convenience. But it also brings big problems for consumer privacy and data safety. All personal, financial and transaction are kept on these platforms, so the risk of data leaks or breaches are a big problem<sup>1</sup>. Data breach means someone gets personal or financial information without permission. If we discuss about E-commerce, it can be name, address, phone number, credit or debit card, bank account, login password or shopping detail which may be used for cause money loss, identity theft, loss of trust and harm to the company name<sup>2</sup>. Many big data leaks happen in India and the world. For example, a 2021 data leak in a big Indian e-commerce website exposed millions of users' information. It shows the problem of the responsibility of platforms to keep data safe. Data breach is not only a problem for the user but also for the law. India has the Consumer Protection Act, 2019, and the Information Technology Act, 2000. These laws give rights to consumers for safety, privacy, and protection from unfair trade. Section 2(1)(o) defines "unfair trade practice," which includes bad data security<sup>3</sup>. Sections 2(1)(r) and 2(1)(d) give consumers the right to privacy and protection<sup>4</sup>. These laws help to hold e-commerce platforms responsible if data leaks happen. But the problem is complicated. E-commerce platforms work as middlemen between sellers and buyers, so it's hard to say who is responsible and decide the accountability. Consumer is asking for more care, due diligence and safety standards. The court says the platform must give strong security, tell the user if a data leak happens and fix the problem quickly by which the loss of the consumer may be reduced and protected. If it fails, the platform can face liability, pay compensation, and get regulatory action. Other country laws also show importance. The EU has GDPR, which provide strict data protection, where

---

<sup>1</sup> Kshetri, N. (2018). *1 The Emerging Role of Big Data in E-commerce*. Communications of the Association for Information Systems, 43(1), 17.

<sup>2</sup> Dey, L., & Bansal, A. (2021). *E-commerce in India: Growth, Challenges and Opportunities*. International Journal of Research in Management & Social Science, 9(2), 1–8.

<sup>3</sup> *Consumer Protection Act, 2019*, Section 2(1)(o), Government of India.

<sup>4</sup> *Consumer Protection Act, 2019*, Sections 2(1)(r) and 2(1)(d), Government of India.

the notification to the user is compulsory if there is a breach and other consumer rights. The USA has CCPA, which makes companies responsible and accountable for data breaches and consumers are safe and having good faith in the laws. If we discuss about India, in India we find some gaps and there is an immediate need to improve laws to protect consumers in the digital market. This paper studies law about e-commerce data breaches in India, especially the liability of online platforms under consumer protection law. It will check how law developed, court decisions, and the duty of e-commerce platforms to keep data safe. It also studies problems in practice, like technology, area problems, and the third-party company role. The paper wants to give a full view of how consumer protection law works in digital risk and check how the law holds platforms responsible. Also, the paper shows a policy problem. Protecting data is a legal duty and a business need. If a platform is not safe for data, it can lose reputation, consumer trust, and market. Good liability law makes platform use strong security, shows transparency, and gives trust to the user. By studying liability under law, this paper connects technology and law so consumer rights are safe in digital shopping<sup>5</sup>. In short, e-commerce changes shopping but gives new risks for privacy and security. Data breach is a big legal and social problem. Need clear responsibility in law. This paper studies the liability of the platform and gives ideas about law, rules, and policy to protect consumers. This introduction gives a base to study law, technology, and consumer rights and shows the importance of responsibility for safe and trustworthy e-commerce.

## **2.HISTORY AND EVOLUTION OF E-COMMERCE DATA BREACHES IN INDIA**

We can understand the growth of E-commerce and the data breach problem by examining its history. Even though online shopping is new concept for consumers but protection is much required. This part looks at the history of law for E-commerce data breaches in India, from old consumer protection law to modern rules and also shows the steps taken towards similar problems in history.

**2.1 Pre-Digital Period: Start of Consumer Protection:** Before online shopping, the idea of consumer protection already existed in India because the protection of consumer is equally important as the business growth. In the early years after independence trade was going mostly in physical markets. People was faced issues related to harmful products, cheating and unfair business. This concern first time led to rules to protect consumers and protect their rights by framing adequate laws. The Consumer Protection Act, 1986, was implemented<sup>6</sup>. It made way for consumer complaints, councils and forums at district, state and national levels<sup>7</sup>. It did not discuss online shopping directly, but it helped hold

---

<sup>5</sup> Information Technology Act, 2000, Government of India

<sup>6</sup> Government of India, *Consumer Protection Act, 1986*

<sup>7</sup> Bansal, A., & Dey, L., *Evolution of Consumer Rights and Online Protection in India*, International Journal of Research in Management & Social Science, 2020, 8(4), 12–20.

businesses responsible for unfair practices. Rules about unfair trade, product defects, and poor services became the basis for protecting consumers in online business. Even then, the focus was on fairness, transparency, and accountability, which later became crucial for online data safety<sup>8</sup>.

**2.2 Early Digital Era: Information Technology Act (2000–2010):** After the year 2000, digital shopping started in India. More people used the internet, online banking, and tech startups. India passed the Information Technology Act, 2000, which made cyber activities legal and illegal. Sections 43 and 66 punished hacking, data theft, and unauthorized access. At that time, the IT Act was more about protecting computers from hackers than protecting consumer data. E-commerce was small, and online shopping was limited. But hacking, phishing, and identity theft started to appear. Such incidents showed the need for special consumer protection in the digital world. Platforms tried security measures like encryption, secure payment, and passwords, but they were voluntary and not the same everywhere. Consumers were still at risk. Law was reactive—it worked after a breach happened, not to stop it before<sup>9</sup>.

**2.3 Growth of E-Commerce and Law Response (2010–2018):** From 2010 to 2018, e-commerce grew very fast in India with Flipkart, Amazon, Snapdeal, and Paytm Mall. Millions of people shared personal and financial info online. Data breaches became more common, showing weak security in platforms. The Consumer Protection Act, 1986 was not enough for digital shopping because it does not cover all E-commerce problems. Courts directed the government to frame appropriate laws by which the rights of the consumers may be protected and court also include right to privacy for the consumers. Courts also said platforms cannot escape from responsibility by saying they are just intermediaries. They must take care of user data. Some important cases came where consumers complained about data leaks<sup>10</sup>. Consumer forums and regulators started holding platforms responsible for weak security, unauthorized sharing of info, and not having proper complaint handling. This period prepared for stronger digital laws<sup>11</sup>.

**2.4 Modern Digital Era: Consumer Protection Act, 2019 and After:** The Consumer Protection Act, 2019, recognized the digital shopping challenge. It defines e-commerce and online marketplaces and their duty as middlemen between seller and buyer. Sections about unfair trade, poor services, and privacy give legal power to hold platforms responsible for data breaches. The 2019 Act asks platforms

---

<sup>8</sup> Singh, R., *Consumer Protection in India: Historical Overview*, Journal of Indian Law & Society, 2015, 6(2), 45–58.

<sup>9</sup> Sharma, S., *E-commerce Security Challenges in India (2000–2010)*, International Journal of Advanced Research in Computer Science, 2011, 2(3), 45–52.

<sup>10</sup> Shreya Singhal v. Union of India, (2015) 5 SCC 1.

<sup>11</sup> Dey, L., & Bansal, A., *E-commerce in India: Growth, Challenges and Opportunities*, International Journal of Research in Management & Social Science, 2017, 5(2), 1–8.

to be clear about terms, security measures, complaint handling, and the responsibility of sellers and platforms. Hon'ble Apex Court and various High Courts directed the concerned authorities to take reasonable steps to protect data. If they fail, they need to pay a penalty of compensation and they have to face regulatory action. Regulators and industry promote proactive safety, not just punishment after a breach they need to take actions which ensure the protection of breach. Global law like GDPR also influenced<sup>12</sup> India to follow world standards<sup>13</sup>.

**2.5 Contemporary Challenges and Continuing Change:** Even now, e-commerce data breaches are a big problem. Platforms must decide responsibility when many parties' handle data—platforms, sellers, or payment providers. Who is responsible is still a challenging legal and practical question. Recent incidents show gaps in law enforcement, weak security, and low consumer awareness. Lawmakers discuss how to balance platform responsibility, tech innovation, and consumer rights. COVID-19 increased online shopping, so data safety is more important. History shows a shift from reactive law in the early IT era to active consumer protection now. Law now not only punishes breaches but also requires platforms to prevent them. Align with global standards and educate users. As e-commerce grows, law will keep evolving to make online marketplaces safe, clear, and responsible.

### **3.LITERATURE REVIEW**

E-commerce data leaks show people's personal and money information. The study gives two main law problems: one is data-protection duties of platforms and service providers under privacy/data law, and the second is consumer-protection liability when leaks cause money loss, cheating, or unsafe services. Indian writers on this topic write in different ways: some show law gaps and enforcement problems, some explain how consumer law and DPDP/IT law can propose solutions, and some present ideas for better rules like strong breach reporting, careful checking, and platform responsibility. Seven Indian writers below show law scenes, review new laws and rules, and provide ideas for reforms to make online platforms more responsible for people.

#### **3.1 Author: Dr. Pavan Duggal, title: Cybersecurity Law & Practice; many articles on data protection, platform duty, and breach rules**

Dr. Duggal, a cyberlaw expert, looks at the duties of online intermediaries and e-commerce from a cybersecurity and law view. He says platforms must do strong checking and incident response and tell users when a breach happens. He shows gaps in the IT Act, and the new DPDP makes it hard for victims of big leaks. Duggal focuses on legal ready work: vendor contracts, must report breaches, and

---

<sup>12</sup> European Union, *General Data Protection Regulation (GDPR)*, 2018

<sup>13</sup> Indian Courts, *Case Examples on E-commerce Liability and Data Protection*, Supreme Court of India, 2020–2023.

remedies in law to make platforms answerable to people. Many lawyers and policymakers rely on his writings as a guide for platform responsibility<sup>14</sup>.

**3.2 Author: Apar Gupta, title: Opinion and articles on India data law and platform duty (Indian Express, Down To Earth)**

Apar Gupta (Internet Freedom Foundation) says DPDP and the rules are vague and do not have enough safe points. He says the law is not clear on breach notice, small remedies for people, and many exemptions, so consumers remain unprotected after platform leaks. Gupta says law must clearly give duty to platforms listing/hosting transactions—not only the seller—so people can get refunds or compensation after data loss. He wants strong law enforcement, clear notice rules, and an independent oversight on platforms<sup>15</sup>.

**3.3 Author: Pranesh Prakash, title: “Data matters: once more, unto the breach,” and other articles on big leaks (CIS / media)**

Pranesh Prakash writes about big leaks (Covid, vaccine, others) and reasons: platforms collect too much data, weak access, and low responsibility. He says without a strong legal duty to tell users about breaches; people cannot know harm or get remedy. Prakash asks for transparency, real breach-notice rules, pressure on platforms for better security, and public interest remedies with consumer claims. His writing mixes reports and policy advice for regulators and civil society<sup>16</sup>.

**3.4 Author: Sunil Abraham; title: Articles and interviews on data protection, government access, and platform duty (CIS/Tech Circle/Press)**

Sunil Abraham says Indian law has not been proper on data security for a long time; platform duty must see privacy and consumer harm. He shows trade-offs—too much government access or bad law writing hurts remedies—and wants rules that make platforms keep consumer data safe and user rights. His work is useful for readers to see the balance between privacy, public interest, and consumer protection<sup>17</sup>.

**3.5 Author: Nikhil Pahwa, title: Media Nama reports and articles on platform data security, DPDP, and e-commerce rules**

---

<sup>14</sup> Pavan Duggal, *Cybersecurity Law & Practice: Analyses on Data Protection, Platform Liability and Breach Obligations* (New Delhi: Pavan Duggal Associates Cyberlaw Consulting, 2023)

<sup>15</sup> Apar Gupta, “Digital Data Protection Bill uses brevity and vagueness to empower government, undermine privacy,” *The Indian Express* (20 November 2022)

<sup>16</sup> Pranesh Prakash, “Data matters: once more, unto the breach” (16 June 2023), *Hindustan Times*,

<sup>17</sup> Sunil Abraham, “Govt access, localisation norms in data protection bill need rethink: CIS, Sunil Abraham,” *TechCircle* (1 August 2018),

Nikhil Pahwa, tech journalist and Media Nama founder, reports policy changes (DPDP Act, draft rules) and real platform leaks. He shows how law timing, gaps, and platform practices affect people after a breach—like if the platform tells users fast or does steps to correct it. His work effectively illustrates the changes in law enforcement and the practical impact of new consumer protection rules on e-commerce<sup>18</sup>.

### **3.6 Author: Advocate Puneet Bhasin, Title: Guides and analysis on DPDP and breach of duty**

Puneet Bhasin (cyberlaw lawyer) writes for lawyers on how DPDP and old IT rules impose platform duty after a breach. She talks about practical compliance—notice time, responsibility split between marketplaces and sellers, and penalty risk—and gives checklists for corporate lawyers. Her work joins law theory with real steps platforms must take to limit loss and protect consumers after a breach<sup>19</sup>.

### **3.7 Author: Anjali Bharadwaj, title: Public interest articles and critique on DPDP and breach of transparency (The News Minute / The Hindu / public writings)**

Anjali Bharadwaj (activist) critiques lawmaking and the effect of DPDP/rules on citizens. She says people need clear breach notice rights and easy complaint methods (consumer forums, CCPA-type actions) to get remedies after platform leaks. She stresses civic checks, public breach reports, and strong consumer enforcement so platforms cannot hide leaks or only depend on contracts<sup>20</sup>.

## **4. ANALYSIS AND DISCUSSION**

E-commerce has changed the way people was buying goods and services in the past. It gives convenience, speed and wide access even here consumer is having twenty-four-hours facilities. But using digital platforms also brings a big risk of data breaches, where consumers' personal information can be stolen, misused, or accessed by the wrong people. A key question is who is responsible when this happens. Under consumer protection law, online platforms have liability, meaning they must be accountable for protecting user data while still allowing business growth and innovation. This part looks at the liability of e-commerce platforms in India, how it works in practice, and what challenges remain.

**4.1 Nature of Liability of Online Platforms:** Online platforms connect buyers with sellers and services, so they have a duty to protect consumer data. The Consumer Protection Act, 2019 provide

---

<sup>18</sup> Nikhil Pahwa, "15 Issues with India's 2025 E-commerce Self Governance Policy," *MediaNama* (30 January 2025),

<sup>19</sup> Advocate Puneet Bhasin, *Digital Personal Data Protection Act, 2023: An In-Depth Analysis* (PuneetBhasin.in, 2023)

<sup>20</sup> Anjali Bhardwaj, "Data Protection Act will limit journalism to PR: Transparency activists," *The News Minute* (27 April 2025)

certain provisions which says platforms shall be held responsible and accountable if they fail in service and including the remedies for not keeping user data safe and secure. Liability comes not only when the platform itself is careless but it also comes when third-party sellers on the platform fails to protect the data of the users. In simple words, platforms cannot say, “We are just a website”; they must make sure user information is secure and they are accountable and responsible as per the statutes. If courts find such matters where platforms are not taking proper steps to prevent breaches then court shall pass orders in favor of the users to maintain the data safe and secure.

**4.2 Duty of Care and Standards of Security:** Duty of care means platforms must take proper steps to protect data not the ignorance shall be there. This includes using tools like encryption, safe payment systems, strong login and other industry-standard security which secure the user data and trust in the concern business or website. The Consumer Protection Act, 2019 says users should not face risks or unfair practices due to the platform’s carelessness and otherwise due to the others mistakes. Further is shall be the duty of the platform authorities, if a breach happens, they must inform users quickly so the user can deal accordingly. Duty of care ensures “platforms cannot ignore security problems” and must act responsibly to prevent harm and safe the user data and privacy.

**4.3 Judicial Precedents and Interpretations:** Hon’ble Courts in India directed via many cases that platforms must protect consumer data, it is the first duty of the platform to maintain the trust and data secure of the user other come after that. Even there are few cases about online breaches, where Hon’ble Courts use the IT Act, 2000 and consumer laws to handle the concern issues and pass the decision in favor of the users to maintain trust and law in the society. Hon’ble Courts settled this principle that platforms are responsible and accountable for service failures even if a third party is involved. Consumers have right to get compensation and can get remedies if data is stolen due to negligence. Courts also directed the government to make certain rules and policies where platforms shall fix security systems and inform users regarding the breach. These decisions show that platforms have a legal duty to protect data under both cyber law and consumer law.

**4.4 Challenges in Determining Liability:** Even with law, holding platforms responsible is not easy. Many actors are involved—sellers, payment gateways, cloud providers—so it is hard to decide who is at fault. Technology changes fast, and today’s secure system may become weak tomorrow. Cross-border transactions create problems because data may be stored in another country, causing legal issues. Many consumers do not know their rights or even that a breach happened, making enforcement difficult. These challenges show the need for clearer rules and security standards.

**4.5 Comparative Perspectives and Lessons:** India can refer other countries rules, policies or legal framework to deal with similar matters because this matter is very serious and need to frame adequate legal framework like- EU's GDPR makes platforms protect data, report breaches fast and get user prior consent, US laws like CCPA give consumers rights to access, delete or control their data, Singapore makes platforms regarding breach, the authorities shall notify users and take appropriate actions as quickly as possible which shall secure the users data and privacy. This suggest us that we should have clear security standards, mandatory reporting and stronger enforcement by which our consumer data shall be secure and safe.

**4.6 Policy Implications and Recommendations:** Growth in E-commerce business shows need to have clear rules to handle user data safe and secure. Government should frame policies which secure the consumer rights and follow maximum security measures to stop breaches. Law should clearly explain or define responsibility and accountability, especially for third-party sellers and duties of the platforms or businesses. Rules for notifying consumers and authorities quickly after a breach are needed. Consumer awareness about rights and data safety is important. Regulators should be strong enough to monitor, investigate, and enforce law. These steps will balance online business growth with consumer protection, making e-commerce safe for everyone.

## **5.SUGGESTIONS AND RECOMMENDATIONS**

These suggestions make a balanced system where platforms or online businesses can work easily while keeping consumer data safe.

**5.1 Clear Legal Framework for Platform Liability:** The first step to protect consumers in e-commerce is to make clear laws about platform liability. Now we are dealing with laws like- Consumer Protection Act, 2019 and IT Act, 2000 gives us a general guidance and understanding about the e-commerce but do not clarify the needs for platforms. Law shall be clear about the platform's duties like- related to protect consumer data, manage third-party sellers matters and secure payments. It will help to stop from misuse and help consumers secure their data safe and secure; it will promote e-commerce.

**5.2 Standardized Security Guidelines for Platforms:** Government shall prescribe certain basic or minimum-security standards for platforms to protect user data safe and secure. Under this we may include strong encryption, secure payments, regular security checks, two-factor login and safe storage of sensitive information and others. These rules shall be similar for all platforms in security, helping regulators check them easily, and give consumers confidence. If a platform breaks rules and a breach

the data of the consumer, it must be held responsible and accountable. Clear security mechanisms rules increase platforms investments in better technology and protect their reputation and goodwill.

**5.3 Mandatory Breach Notification Rules:** Government shall make this compulsory for the platforms to notify the consumers and appropriate authorities quickly as earlier as possible if a data breach happens. Because it helps users take safety steps like changing passwords, freezing accounts or monitoring transactions and other required steps. Appropriate authorities shall take actions by which the data of the consumer may be protected. India can refer the other countries legal framework to deal such and similar matter like EU's GDPR, which requires notice within 72 hours. Mandatory notice rules give transparency, responsibility and faster response to breaches which will reduce consumers loss and promote e-commerce, also built and increase the trust of the consumer in e-commerce.

**5.4 Strengthening Regulatory Oversight:** The Government shall frame such policies where a strong regulatory supervision shall be for e-commerce platforms. Regulators can check platforms' security, investigate breaches and notify the appropriate authorities for decide penalties if needed. Special units in consumer authorities can handle cyber complaints, check damages and guide consumers to protect data secure and prevent from such breaches. Regular checks and audits will build trust of the consumers; it may increase the amount of consumer towards e-commerce. Strong legal framework makes platforms accountable and liable before such issues or problems arrive not after a breach. It will reduce negligence cases as well as other cases and gives better protection to consumers and promote e-commerce platforms, built more trust towards these platforms.

**5.5 Consumer Awareness and Education:** Consumers are very important for every business. Consumer should aware about their rights, risks and how to prevent from problems. Awareness campaigns can teach consumer to make strong passwords, not share sensitive info and check website security before buying, it will help consumer for better understanding as well reduce the pain of the businessmen. Educated consumers can handle breaches in a better way that may reduce loss and demand accountability from platforms or from the third party. Government shall come up with compulsory training programs then industry and platforms shall organize campaigns through social media, announcements and training. Knowledgeable consumers always make e-commerce safer and reduce data breach risk, help in growth of the business because one case may affect goodwill of the platform.

**5.6 Collaboration with International Best Practices:** Center Government should refer other countries rules, policies and legal framework regarding this matter which may help for better

understanding, not only that we should collaborate with foreign countries and grow business and relations at international level.

## **CONCLUSION**

E-commerce has become a basic part of our daily life, it gives consumers easy access, choices and convenience but with these benefits it also comes with certain issues like the responsibility of keeping consumer data safe. Now a days data breaches becomes the normal case because we do not have appropriate laws which may deal accordingly. We should come up with the legal framework, so that consumers can shop online without fear of misuse or carelessness. Consumer Protection Act, 2019 and IT Act, 2000 provide certain provisions for protection to consumers, but they do not clearly explain exactly what online platforms must do in case of a data breach. Platforms shall be held responsible and accountable for unfair practices and provide with specific provisions related to security measures, reporting breaches or third-party matters. Currently we do not have such policies which may deal accordingly and due to this it creates delays in solving problems related to negligence matters. Consumers have the right to claim remedies if their information is leaked because of platform negligence or because of third-party service providers. Technology is changing more faster, cyberattacks get smarter and we are unable to resolve such issues. This shows the importance of immediate legal framework, policy which may decide deciding responsibility and accountability for breach and other e-commerce matters. Looking at other countries shows India needs clear rules. The EU with GDPR makes platforms secure data, report breaches fast and obtain user consent. The USA with CCPA provides consumers control over personal data. Singapore requires rapid reporting and corrective action. These countries show that clear laws, active enforcement and informed consumers are key to reducing data breach risks. The suggestions in this paper show a multi-step approach. Consumer trust is the foundation of digital markets; repeated breaches can reduce trust, slow growth, and harm the economy.

## DNA PROFILING AND PRIVACY IN INDIA: A CRITICAL APPRAISAL OF THE 2019 DNA REGULATION BILL AND NEW CRIMINAL LAWS WITH COMPARATIVE PERSPECTIVES FROM THE USA, UK AND EU

Tanu Gupta \*  
Vinod Kumar\*\*

---

### ABSTRACT

The research paper examines the legal, constitutional, and the human rights aspects of the proposed DNA Technology (Use and Application) Regulation Bill in India. It addresses two major issues. First, this paper will focus on whether the Bill is compatible with the fundamental right to privacy as established by the Supreme Court in the landmark Justice K.S. Puttaswamy case, which identifies privacy as a constitutionally ensured right. Gathering and application of genetic information should fulfil stringent conditions such as necessity, proportionality, and legal protection to prevent breach of privacy. This paper outlines precautions that must be incorporated in the Bill to curb abuse of DNA information. Such safeguards include high standards of consent regime, restrictions on data retention and use, independent supervision and a definite right of individuals to object against unreasonable inclusion of genetic data concerning them. The paper also recommends that the DNA Bill must be harmonized with the general privacy laws including the Digital Personal Data Protection Act, 2023 so that the right of the citizens is fully secured. Despite the promise of DNA technology on the justice and identification front in India, it has its threats in the future particularly when uncontrolled. Therefore, a serious restraint is required in addition to an imperative demand to defend the right in law, dignity in man as well as safeguard constitutional values in the handling of delicate genetic material. This article brings out the fact that responsible use, and control of DNA technology can encourage justice and privacy in a framework of a dynamic legal landscape in India.

**Keywords:** DNA Technology, Regulation Bill of 2019, New Criminal Laws 2023, Forensic Evidence, Comparison of Legal Framework with India, etc.

---

\* Research Scholar, Amity Law School, Amity University Jaipur, Rajasthan

\*\* Associate Professor, Amity Law School, Amity University Jaipur, Rajasthan

## 1. INTRODUCTION

Within the past few decades, DNA technology has been one of the most important aspects of the legal and criminal justice system in India. Previously applied in limited instances, DNA profiling is being consistently utilized in law enforcement activities as well in locating missing individuals and in civil law proceedings where there are differences of paternity and challenges to inheritance. The value of the DNA evidence is based on the fact that it is very reliable provided it is successfully handled, and thus it is possible to convincingly associate the suspects with crime scenes, it has assisted in freeing the wronged and ultimately resolve cold cases. It is used in the investigation of serious crimes, such as rape, murder, and mass disasters, through to most everyday issues relating to personal identity and family issues.

The increase in the application of DNA profiling has been rapid but without appropriate control. India is presently experiencing a very wide gap in policy regarding the collection, storage, use, and protection of DNA data.<sup>1</sup> Despite the DNA evidence being admitted in court as a general scientific expert testimonial, yet it lacks the specific act detailing the manner of preserving the samples, retention of profiles, and the maintenance of sensitive data of the citizens, confidential and secure. To fill this regulatory gap, the DNA Technology (Use and Application) Regulation Bill was initially proposed in 2019. It had objectives of introducing a national DNA database, the formation of a DNA Regulatory Board and stipulating standards of labs and investigators.<sup>2</sup>

However, this absence of a statutory framework has given rise to several concerns. In the absence of rules, it is possible that the DNA information might be falsely handled or abused. As an illustration, DNA can be stored without appropriate consent, particularly, on people who committed less serious crimes or got into civil litigations, and this can be a challenge to privacy and infringement of the rights of individuals. The absence of supervision in the storage of the DNA profiles may increase the risk of being falsely indexed in criminal databases, discrimination, and/or possible theft of leakage of such intensely personal data. Supreme Court caselaw and legal commentary, especially regarding high-profile cases, have insisted on powerful safeguards against violation of fundamental rights such as privacy, autonomy, and due process in the name of efficient justice.

---

<sup>1</sup> S Panneerchelvam and MN Norazmi, 'DNA Profiling in Human Identification: From Past to Present' (2023) 30(6) Malaysian Journal of Medical Sciences 5 <https://doi.org/10.21315/mjms2023.30.6.2> accessed 1 December 2025.

<sup>2</sup> The DNA Technology (Use and Application) Regulation Bill 2019, Bill No 128 of 2019 (India), introduced in Lok Sabha on 8 July 2019.

This paper discusses the issues of legality, constitutionality, and human rights of the proposed DNA Technology (Use and Application) Regulation Bill. It is concentrated around two prominent questions, the first one is whether the Bill is in conformity with the constitutional right to privacy, particularly as the Supreme Court has decided in *Justice K.S. Puttaswamy v. Union of India*, in which it was established that privacy was a fundamental right.<sup>3</sup> According to the strict standards such as necessity, proportionality and legal protection, any gathering and utilization of genetic information must be subject to rigorous criteria. Secondly, the paper considers protections that should protect against DNA information being used in abusive ways, such as, Publication of note agreements to consent to provision data by highly protective consent regimes and restrictions on retrenchment dumping of data and usage data, independent review and privilege to false or wrongful listing. It also underscores the urgency of ensuring that the DNA Bill in line with broader privacy rules like Digital Personal Data Protection Act, 2023 to protect citizens rights. Thus, then, the DNA technology offer a remarkable promise for enhancing justice and identity in India, but it also has severe potential downsides if not properly regulated. It is not only a necessity but also an emergency for every time the genetic data are involved, promotion of legal rights and human dignity and constitutional values need to be ensured.<sup>4</sup>

## **2. UNDERSTANDING DNA TECHNOLOGY IN LEGAL CONTEXTS**

The application of DNA technology especially DNA profiling has become a significant aspect of the contemporary legal system. DNA profiling is also referred to as the process of identification of an individual by analysing his or her unique genetic makeup. The DNA structure is unique in any person except identical twins and therefore is an exceptionally efficient method of connecting people with biological material such as blood, hair or skin cells left behind at the crime scene. In law, DNA profiling is a widely used technique in the criminal investigation. It helps the police to link a suspected individual to a crime scene, prove or disprove their presence and to even find out unidentified victims. An example is the case of rape and murder, whereby the DNA sample taken out of the victim body can be compared and matched with that of the suspect to verify the involvement. Similarly, in cases where there is a suspect, DNA can be utilized to clear the innocent and demonstrate the other suspects guilty and this can be used in averting wrong convicts.

The other important use of DNA technology in the legal process is in field like in the paternity and family law proceedings. In custody cases, child support cases or succession cases, DNA testing can be

---

<sup>3</sup> Government of India, Ministry of Law and Justice, *The Constitution of India* (as on 1 May 2024, Legislative Department, Official Languages Wing 2024).

<sup>4</sup>The Indian Express, 'Explained: What Is the DNA Bill?' <https://indianexpress.com/article/explained/what-is-the-dna-bill-8857810/> accessed 10 December 2025.

applied to identify a biological connection especially between two people. It is in this regard that the court relies on such scientific evidence to dispose emotionally and legally complex family cases. DNA profiling is also useful during disaster cases when it is difficult to identify the dead bodies because of excessive damage. The DNA testing helps the authorities in identifying people involved in natural disasters like earthquake or manmade disasters like building collapse or fire in order to provide remains of the victims to their families. This does not only provide a closure to the loved ones but also has a legal connotation in regards to other issues like insurance claims, and succession rights. Similarly, close relatives DNA sample can be cross-examined, in order to determine identity with the unidentified body or person in case of missing persons. This application is especially applied when the case at hand incorporates child trafficking or child abductions or the case that has taken years before it is resolved.<sup>5</sup>

DNA profiling is an effective technique, but it has associated concerns as well. The threat of abuse or falsification is one of the most important issues. In comparison, DNA collection or storage can be incorrect, samples may be contaminated, or the results may have been misinterpreted leading to wrongful conviction/ arrests. In addition to this, the presence of the DNA of an individual in a database introduces the privacy concern, whereby, in case the information is stored forever or utilized in an unforeseen manner, then this constitutes a violation of privacy. Another problem is psychological and social stigmatization. To illustrate, it can damage an ideology, ties and mental well-being of an individual since the wrongful accusation of the individual can be conveyed during the course of a criminal investigation because of a DNA mistake. These incidences combined above are the reason why the legal force must be strong enough so that there can be just, ethical and transparent applications of DNA evidence.

DNA profiling has been used in a number of high-profile cases in India. In the Nirbhaya gang rape case of 2012, DNA was used in supporting the accusations against the accused since their test results were also present in the victim. Mass disasters like train accidents or floods where the visual identification process has been impossible have also been identified using DNA testing.

Thus, DNA technology has revolutionized legal systems with regards to major investigation and personal identification. Although it has scientific soundness and useful information, its application should be weighed on privacy, approval, and human right. The necessary regulation, ethics and quality control are the means to make sure that DNA profiling is used in the interest of justice and without harm.

---

<sup>5</sup> S Panneerchelvam and MN Norazmi, 'DNA Profiling in Human Identification: From Past to Present' (2023) 30(6) *Malaysian Journal of Medical Sciences* 5 <https://doi.org/10.21315/mjms2023.30.6.2> accessed 1 December 2025.

### **3.KEY FEATURES OF THE DNA TECHNOLOGY (USE AND APPLICATION) REGULATION BILL, 2019**

The enactment of the DNA Technology (Use and Application) Regulation Bill, 2019 can be held as a major milestone towards the control of DNA profiling in India. With DNA evidence increasingly being used in criminal and civil cases, a strong and urgent indication to use this form of strong technology appropriately, responsibly, and ethically is needed. This Bill aims to establish an elaborate framework of laws that would govern collection, analysis and storage of DNA samples but would at the same time safeguard the rights and privacy of an individual.<sup>6</sup>

The Bill is proposed to set standard procedures concerning DNA technology to identify individuals, which is one of the primary goals of the legislation. Its purpose is to aid criminal investigations as it assists in the determination of suspects or the innocence of mistakenly accused individuals. It also permits the use of DNA profiling in civil cases, including dispute of paternity, tracing missing persons and identification of unidentified or deceased persons. Not just efficient resolution of crimes and civil matters, the Bill also focuses on the necessity of attention to personal privacy and consent.

The Bill applies in both criminal and civil cases. Within the criminal setting, DNA profiling proves to be useful in indexing recidivists or in connecting an alleged perpetrator to a crime location. DNA may also be utilized in civil contexts to prove biological relationship, help with immigration related confirmation, and find children or people lost in a family in the case of a natural disaster, trafficking, etc. In this way, the Bill gives a general framework to be used to deal with a variety of legal situations in which DNA evidence may have a central place.

In order to store and distribute DNA information effectively, the Bill suggests the formation of a National DNA Data Bank, and a number of Regional DNA Data Banks.<sup>7</sup> The duty of these data banks will involve the storage of DNA profiles that have been obtained through numerous services such as crime scenes, suspects, convicts, undertrials, missing persons and dead bodies that have not been identified yet. Through a systematized way of storing this information by categorization, the authorities will be capable of matching profiles faster and faster with greater accuracy, hence giving a faster and more accurate investigation.

---

<sup>6</sup>supra note 4

<sup>7</sup> PRS Legislative Research, 'The DNA Technology (Use and Application) Regulation Bill, 2019' <https://prsindia.org/billtrack/the-dna-technology-use-and-application-regulation-bill-2019> accessed 12 December 2025.

One of the major aspects of the Bill constitutes the formation of a DNA Regulatory Board to be the primary source of oversight services on the issue of DNA throughout the country. The Board will comprise of experts across disciplines in molecular biology, law, police services, and forensic science as well as by central government representatives. Among them will be to grant and check DNA laboratories, regulate that the professionals within it act according to ethics, certify specialists, and see that DNA data is maintained suitably and safely. The presence of the Board is significant in order to ascertain the transparency and accountability of the employment of DNA technology.<sup>8</sup>

The Bill also describes how consent should be acquired during the collection of DNA. In civil suits written consent of a person must be obtained before obtaining their DNA. It is however different in criminal cases. Consent is not needed in the collection of DNA in cases where the offence carries a punishment other than seven years imprisonment or when death penalty has been provided in the offence. When it comes to minor offences, consent of the individual is required. In case of refusal of consent, the investigating officer should record the refusal in writing and then he should seek the approval of a magistrate and then proceed. This framework tries to create a balance between the need of investigation and individual right to privacy.

The Bill also states penalties against misuse or mishandling of DNA data to prevent this possibility. In case an individual deliberate shares or leaks confidential DNA, he/she will be put behind bars with the tenure not exceeding three years or pay a fine of not more than 1 lakh without an exception of such an individual. Violations of unauthorized access to DNA databases and any kind of tampering with DNA samples are also punishable in the Bill. The development of these legal protections is aimed at encouraging the spirit of confidence and responsibility with regard to the application of DNA technology.

The ultimate objective of the Bill lies in utilising the tool of DNA profiling as a method of precise identifying. DNA will ascertain that an individual was or was not present as a crime was committed to prevent wrong convictions. It aids also in the confirmation of family relations, locating missing persons, body identification when identification using the eye alone is not possible. Through these benefits, the Bill would introduce uniformity and scientific precision to genetic testing within the context of Indian justice. thus, its application should be ethical in its approach, where the rights and privacy of individuals cannot be compromised to the ideologies of advancement.<sup>9</sup>

---

<sup>8</sup> Supra note 4

<sup>9</sup> Vaishali Gupta, 'New Genetic Technology in Legal Arena: A Critical Study of the DNA Technology (Use and Application) Regulation Bill, 2019' (2021) 9(4) *International Research Journal of Commerce and Law* 11.

#### **4. CONSTITUTIONAL ANALYSIS**

The DNA Technology (Use and Application) Regulation Bill, 2019 has become one of the key legal debates with respect to fundamental rights relating to the right to privacy.<sup>10</sup> This issue received a lot of traction with a notable judgment of the Supreme Court in the case of Justice K.S. Puttaswamy v. Union of India (2017)<sup>11</sup>, in which the Court unanimously affirmed that the right to privacy is a fundamental right under the Article 21 of the Indian Constitution.<sup>12</sup> It was stated in this ruling that privacy is not only the right to be left alone but also keeping a person in control over his or her personal information, and informational privacy, specifically, is very applicable in modernity, where there are digital technologies and biological data.

DNA as a variety of personal data is the highest sensitive type of data, providing the information about the identity, family, health status, and genetic peculiarities of a person. Whether it is used or kept, the use of DNA is a highly personal matter and, therefore, its improper storage and use can cause a significant threat to the privacy right. Puttaswamy judgment provided a clear guideline to determine the intrusion in the Article 21 of the constitution whether there is the intrusion into the privacy that is constitutionally acceptable by the state. This criterion has been referred to as the test of proportionality and it has four major tests which are that the action should be approved by law and that it should have arguably a worthy aim and that it should also be necessary in a democracy and the invasion should be commensurate to the purpose of the invasion itself.<sup>13</sup>

When this test is applied on DNA Bill, there are strengths and weaknesses which can be observed. The Bill does have a framework of law that underpins its application, and the intention behind this-improvement of criminal investigation, and the establishment of persons in civil litigation cases is a questionable one. However, questions of whether the procedures employed are not disproportionate and whether the actions are timely are up in question to ensure that the scope of infiltration in people chains become excessive. The Bill will facilitate very extensive proliferation and retention of DNA profile of individuals who have not been convicted since they are only suspects or under triers. This presents a risk of going against the fact that individuals ought to be innocent until the time they are

---

<sup>10</sup>PRS Legislative Research, 'The DNA Technology (Use and Application) Regulation Bill, 2019' (2023) <https://prsindia.org/billtrack/the-dna-technology-use-and-application-regulation-bill-2019> accessed 15 December 2025.

<sup>11</sup> Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

<sup>12</sup> Government of India, Ministry of Law and Justice, *The Constitution of India* (as on 1 May 2024, Legislative Department, Official Languages Wing 2024).

<sup>13</sup> IY Brain, 'A Critical Analysis of the DNA Technology (Use and Application) Regulation Bill, 2019' (2023) *International Journal of Law* 467.

found guilty. According to the principle of proportionality, there is something wrong with keeping the DNA profiles of non-convicted persons, still not even of individuals who have accepted the provision of their profiles under dubious or curative terms.

Consent, which forms the centre of the respect of privacy, is treated erratically in the Bill.

The Bill requires consent to the collection of the DNA in civil case but not in the criminal case. The consent is not required in the case of serious crimes (the crimes that are punishable by a sentence more than seven years or death penalties). In other circumstances, a request of permission is sought but in case of a refusal, the investigating officer has the right to seek the permission of a magistrate to proceed. This creates a loophole especially on lower trials and suspects since they are not aware of their rights, or may be pressured to sign. There is also no question of the right of a particular individual to withdraw consent at a later stage or to request the deletion of their DNA data even in case of acquittal or finding them to be innocent.

Another great matter of concern is the absence of specific and extensive protections against civil collection of DNA. Sensitive data can be collected in matters of civil character e.g., paternity disputes, ownership of family properties or finding missing individuals which is not specified in the Bill with regard to privacy protection. As an example, no strict regulations concerning the storage period of the DNA data in civil cases and their manner of destruction following the completion of their goal exist. Unless there are stern laws regarding the storing, retaining and removal there are chances that the DNA information will be abused in some way, it will be leaked or may even be used in an unintended manner.

The other significant problem is the risk of blanketed surveillance and profiling, especially against the minority groups. The Bill authorizes the creation of large national and regional DNA databases. The fact is that these banks are established to assist in the crimes and finding people who are lost, and simultaneously it brings about the chances of the mass acquisition of data on separate populations. This can become the over-representation of certain groups such as the Dalits, Adivasi, migrants or the minority group unless critical checks are established. Institutional prejudice and discrimination and even wrongful arrests can be brought about by such systemic targeting. It has been proven that the existence of DNA databases in the world can easily be abused through surveillance and community profiling or even occurrences of political abuse unless properly controlled.

The Bill also lacks excellent independence of check and redress. The suggested DNA Regulatory Board may not be accountable and independent as it is expected to control the data banks and laboratories. Individuals, who provide the sample of DNA, do not observe a particular method of

attracting, rectifying data or submitting complaints regarding abuse. The information itself is also rather non-transparent in terms of who is to access it and why that, depriving the state and individuals of a balance of power.

All these issues being discussed, it is realized that the DNA Technology Bill is beneficial to the society and is not effective in protecting the constitutional rights and this in particular the right to privacy. It is necessary to add more safeguarding benefits as a procedure, more informed consent, especially in the case of the vulnerable, and autonomous controls to enforce proper execution of the regulatory process in accordance with a constitutionally valid approach in a case of Puttaswamy. It should also adopt the principle of data minimization where all the data that should be collected should be done only when the need arises and when the goal is achieved then the data should be disposed.

Thus, DNA profiling<sup>14</sup> is a tool that can contribute to the delivery of justice to an extent but you need to be cautious. Any encroachment upon such personal data that go far deep into the belly of an individual must be legal, restricted, and equitable as is the norm of a constitutional democracy.

## **5. ETHICAL CONCERNS AND GOVERNANCE CHALLENGES**

There are a number of ethical and governance issues whose seriousness is magnified by the proposed application of the DNA technology in the criminal justice system in India under the DNA Technology (Use and Application) Regulation Bill, 2019. The fundamental issue of ethical considerations is about bodily autonomy. Getting biological samples (blood, hair, saliva etc.) of persons can be a common way of the DNA being collected to serve as a means of identification. The procedure can be executed without the explicit consent especially when it is taken to serious crimes. It may be considered as an infringement of the right of an individual to make decisions regarding his body. This case was more threatening considering the scenario of the Indian constitutional rights including the right to privacy and the right to against self-incrimination which is the inseparability of individual freedoms.

The concept of genetic determinism is also morally disturbing. They fear that DNA profiles are not merely utilized in identification of individuals, but it could be construed or applied to make assumptions about an individual capacity, behaviour and medical conditions, even the possibility that somebody is more or less prone to commit specific acts. In the event of such genetic information being accessed or interpreting it wrongly by the authorities, it can even be used as the evidence of upholding

---

<sup>14</sup> BR Mourya, 'The Role of DNA Profiling Evidence on Criminal Justice System in India' (2021) <https://doi.org/10.13140/RG.2.2.17246.46402> accessed 16 December 2025.

the stereotypes or prejudices, which is what makes the threat of treating people as the stigmatized or the whole population.

There is some fear associated with the caste or community profiling that may happen, which ought to be considered as one of the concerns in the Indian prospect. India is defined as a highly complex societal fabric hence people fear that in the event of constructing large DNA databases and their application, the underprivileged groups will be their target. The available statistics at the National Crime Records Bureau already point to the situation in which Dalits, Adivasis and Muslims taken proportionately large numbers in the undertrial population in the country compared to their status in the general population. When the DNA databases filled are dominated with the data of the same groups, there comes a real possibility of reinforcement of social inequalities by the technology or its misuse through discriminative surveillance and targeting.<sup>15</sup>

The other significant ethical and practical issue is data security. Data stored in DNA is very secretive and it may be utilized to reveal personal facts concerning a person like health and family history. The compromise of DNA databases and the loss of the information by hacking, careless storage, and uncontrolled access to the databases by the states or commercial organizations is a real threat. Such kind of leak can result in abuse of the genetic information whether commercial, investigation or even politically. Other countries have given historical examples in the past that unless the right measures are established, highly sensitive information can be shared or sold in ways that could prove to be harmful to people and families.

These are high-stakes risks and thus there is high need to have strict ethical codes and regulatory structures. To minimize risks of misuse, it is essential to implement data minimization principles, i.e. gathering and storing the lowest amount of genetic data strictly required by the narrow purpose of the law underpinning the use of the data. Besides this, transparency must exist in every DNA data collection, storage, analysis, sharing and, lastly, deletion systems. The DNA collection of people must enlighten the individuals about their rights, why the information is used, and where to make an appeal or redress.

The protection laws ought to be clear as to who ought to access the DNA data, what they ought to use and to what extent so that the use of DNA technology in seeking justice is realized without infringing the civil liberties of individuals. Ethicists and representatives of vulnerable populations would have to be included in accountability structures and independent overseeing agencies. Ultimately, at the point

---

<sup>15</sup> Rebant Juyal, 'Regulation & Use of DNA Profiling in India' (2021) 2 *Queen Mary Law Journal* 36 <https://doi.org/10.26494/QMLJ3940> accessed 18 December 2025.

where the debate about the DNA Bill is raging in India, what does matter the most is that the other face of any technology is the question of whether it is ethical and whether the promotion of such activity is brought into the strong-public debate particularly when it comes to such a personal and profound aspect as an individual genetic code.

## **6. LEGAL REFERENCE FOR DNA & FORENSIC EVIDENCE UNDER THE NEW CRIMINAL LAWS IN INDIA**

In 2023, India experienced a massive shift in its criminal justice system as it introduced three new laws abolishing old colonial-era laws that were used to govern India. The Indian Penal Code, 1860 was substituted by the *Bharatiya Nyaya Sanhita, 2023 (BNS)*<sup>16</sup> whereas the Code of Criminal Procedure, 1973 was replaced by the *Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS)*<sup>17</sup>. Also, the *Bharatiya Sakshya Adhiniyam, 2023 (BSA)*<sup>18</sup> which was previously known as the Indian Evidence Act, 1872. Collectively, these reforms brought a more scientific and modernized way of doing criminal investigations and evidence, such as a greater focus on DNA technology and forensic equipment.<sup>19</sup>

In the former legal system, like under Sections 53<sup>20</sup> and 53A<sup>21</sup> of the CrPC, bodily samples such as hair, blood and swabs of semen were to be taken to identify DNA profile especially in the incidences of severe crimes, such as those that resulted in rape cases. Likewise, Section 164A captured the process of medical examination of victims of sexual offences, sampling of biological samples by the investigating officer to enable forensic analysis of such sample.<sup>22</sup> In Section 45 of the Indian Evidence Act, 1872, the opinion of the experts, such as DNA experts, could be presented and the opinion could be reached as a part of the judicial proceeding.<sup>23</sup>

The 2023 version of the BNSS is an extension of these provisions, they are even more detailed and in line with the modern concept of a forensic. Section 349 of the BNSS which is equivalent to the earlier Section 53 clearly legalizes the collection of DNA samples and other body substances of arrested or

---

<sup>16</sup> Government of India, Ministry of Home Affairs, *The Bharatiya Nyaya Sanhita, 2023* (Government of India Press 2023) [https://www.mha.gov.in/sites/default/files/2024-04/250883\\_english\\_01042024.pdf](https://www.mha.gov.in/sites/default/files/2024-04/250883_english_01042024.pdf) accessed 20 December 2025.

<sup>17</sup> Government of India, Ministry of Home Affairs, *The Bharatiya Nagarik Suraksha Sanhita, 2023* (Government of India Press 2023) [https://www.mha.gov.in/sites/default/files/2024-04/250884\\_2\\_english\\_01042024.pdf](https://www.mha.gov.in/sites/default/files/2024-04/250884_2_english_01042024.pdf) accessed 20 December 2025.

<sup>18</sup> Ministry of Law and Justice (Legislative Department), *The Bharatiya Sakshya Adhiniyam, 2023* (Government of India Press 2023) [https://www.mha.gov.in/sites/default/files/2024-04/250882\\_english\\_01042024\\_0.pdf](https://www.mha.gov.in/sites/default/files/2024-04/250882_english_01042024_0.pdf) accessed 21 December 2025.

<sup>19</sup> The Indian Express, 'Criminal Law Bills: Bharatiya Nyaya Sanhita—Key Changes and Highlights' (2024) <https://indianexpress.com/article/india/criminal-law-bills-bharatiya-nyaya-sanhita-key-changes-highlights-9077165/> accessed 22 December 2025.

<sup>20</sup> Code of Criminal Procedure 1973, s 53 (Examination of accused by medical practitioner).

<sup>21</sup> Code of Criminal Procedure 1973, s 53A (Examination of person accused of rape by medical practitioner).

<sup>22</sup> Code of Criminal Procedure 1973, s 164A (Medical examination of the victim of rape).

<sup>23</sup> Indian Evidence Act 1872, s 45 (Opinions of experts).

accused people and therefore clearly approves DNA testing as a valid investigative method.<sup>24</sup> In sexual offences, the Section 360 of the BNSS that superseded the previous limits in Section 164A is concerned with how victims are examined including the obligatory collection of biological sample materials to conduct DNA Tests.<sup>25</sup> This tells the significance of forensic evidence in proving the statement of the victim and the need to achieve justice.

The Bharatiya Sakshya Adhinyam, 2023 has a critical role to play as far as admissibility in court is concerned. The use of expert evidence is further elaborated in Section 37 of the BSA which has substituted the earlier Section 45 of Indian Evidence Act.<sup>26</sup> It has clearly defined the forensics experts and DNA analysts and it has to be made sure that their views are held to be credible and can be touched upon in criminal courts. This development strengthens the credibility of scientific truth and helps the courts to make correct judgments using advanced forensics techniques.

Besides these, another big move was the Criminal Procedure (Identification) Act, 2022 that had made a big step forward in the way its data was being collected already. The Act superseded the Identification of Prisoners Act, 1920, and empowered law enforcers to take biological samples, which could include DNA, of the convicted and arrested persons. It was a step towards the general sense of wider forensic provisions that were already incorporated in the BNSS and BSA since it flows with the regulatory purposes stated in the DNA Technology (Use and Application) Regulation Bill 2019.<sup>27</sup>

All these new laws together make the legal system in using DNA evidence stronger and less opaque. It is in this regard that the BNSS makes building a case, by its clear provisions of how and when DNA profiling samples can be collected, an imperative. The BSA guarantees that such evidence, as provided by experts, is admissible under the law, and the previous laws such as the Criminal Procedure (Identification) Act, 2022 give procedural clarity concerning the ethical metadata in the collection of samples.

Such reforms are an informed move to bring the forensic science into the legal system of India in a systematic, responsible and ethically responsible way. The new laws bring the old provisions on the same line with the prevailing scientific discoveries and close the gap in between the science and the procedure of judicial trial. They are also supportive of the will of the 2019 DNA Bill which was meant

---

<sup>24</sup> Bharatiya Nagarik Suraksha Sanhita 2023, s 349 (Magistrate's power to order specimen signatures, finger impressions, handwriting or voice samples).

<sup>25</sup> *Bharatiya Nagarik Suraksha Sanhita* 2023, s 360 (Medical examination and collection of biological samples in sexual offence cases).

<sup>26</sup> *Bharatiya Sakshya Adhinyam* 2023, s 37 (Expert evidence, including DNA analysts and forensic experts).

<sup>27</sup> *Criminal Procedure (Identification) Act* 2022 (authorising the collection of biological samples, including DNA, from convicted and arrested persons).

to provide certain legal control of the DNA profiling besides offering an appropriate oversight infrastructure.

Therefore, the 2023 legal reform strengthens the legal framework of gathering, analysing, and using DNA evidence. Section 349 of BNSS, section 360 of BNSS and section 37 of BSA support the right of DNA sample of the accused persons, rights of the victims being subjected to medical examination with preservation of DNA samples and admissibility of the DNA evidence as an expert witness of the court respectively. They collectively render forensic science more feasible and support legal safeguards and comply with the constitutional provisions. These are the key milestones towards scientific integrity, respecting the individual rights, and improving the quality of justice in the Indian legal system.

## **7. COMPARISON OF LEGAL FRAMEWORKS OF DNA IN INDIA FROM USA, UK, EU**

Regarding the regulation of DNA technology and genetic information, the United Kingdom, the United States, and the European Union members have established comprehensive legal provisions that can be studied as an example. This overseas experience proves that laws could be formulated in such a way that it ensures that the DNA profiling is subjected to the end that it serves the people in general, and individuals in the same breath, the need to enjoy their privacy, and personal right is not abused. Such frameworks can come in handy in informing the need to balance the two which are being investigated and privacy in the case of India who are only beginning to establish their own DNA laws.

In the United Kingdom, the regulation of DNA databases changed tremendously due to criticism on the part of the population and judicial action. The National DNA Database established in the UK in 1995 was expanding fast, however, it was met with criticism regarding the storing of DNA samples of individuals who were not convicted of a crime.<sup>28</sup> The challenge of this practice was a case in the European Court of Human Rights, the famous case *S. and Marper v. United Kingdom*<sup>29</sup> case, where the Court upheld that indefinite retention of DNA samples of innocent people contravened the right to privacy. Consequently, stringent rules were introduced through the Protection of Freedoms Act, 2012 enactment in the UK. Now DNA samples of individuals who have not been convicted can be deleted from the database whereas individuals who have been convicted of serious crimes have their profiles retained longer. It is overseen by the office of the Biometrics Commissioner, reviewing database practices, enforcing deletion as required and ensuring police adherence to the law. The UK model

---

<sup>28</sup> AO Amankwaa and C McCartney, 'The Effectiveness of the UK National DNA Database' (2019) 1 *Forensic Science International: Synergy* 45 <https://doi.org/10.1016/j.fsisy.2019.03.004> accessed 26 December 2025.

<sup>29</sup> *S and Marper v United Kingdom* [2008] ECHR 1581.

emphasises proportionality that is DNA must only be collected and stored when it is a real necessity with effective systems in place to safeguard and audit usage.<sup>30</sup>

The regulation of DNA data is under a combined federal-state regulation in the United States. The FBI operates a system known as the *Combined DNA Index System (CODIS)* which connects state-to-state DNA databases.<sup>31</sup> There are however various state regulations regarding who may consent to their DNA being collected and how long it may be held. In most cases, DNA is collected on individuals who are convicted of serious crimes and in other states, one who has been arrested of the same crime. The U.S. model consists of expungement statutes so that when someone is not convicted or a case is dismissed, he or she is permitted to demand that his or her DNA is expunged, which may be a complicated procedure and may necessitate litigation. The DNA Identification Act of 1994 prohibits DNA data to be used by any means other than law enforcement such as use of that information in insurance, employment or research. Misuse comes with criminal charges and regular state and federal authorities go round to ensure compliance with these standards. On the whole, the U.S model tries to achieve the safety of the population without being so invasive of privacy in restricting DNA uses, access by people and conditions of storage.<sup>32</sup>

The European Union GDPR encompasses some of the strictest pieces of legislation to protect personal information, which also includes genetic information. The GDPR treats DNA as special category data, and thus it needs increased protection standards<sup>33</sup>. DNA is only allowed to be gathered in circumstances of legal, medical or public interest and individuals shall provide reasonable and informed consent. Individuals also receive information about the motive behind their DNA being collected, storage length, and how they can access their information, ability to correct or delete information. The GDPR encourages data minimisation that ensures that only the required volume of information is retained and the retention of such information is not beyond the necessary period. In case of handling genetic data in a wrong manner, people will also be at a position to make complaints to independent data protection authorities. To the extent feasible, personal identifying information in

---

<sup>30</sup> Aaron Opoku Amankwaa and Carole McCartney, 'The UK National DNA Database: Implementation of the Protection of Freedoms Act 2012' (2018) 284 *Forensic Science International* 117 <https://doi.org/10.1016/j.forsciint.2017.12.041> accessed 27 December 2025.

<sup>31</sup>Federal Bureau of Investigation, *CODIS Audit Report* (September 2001) accessed 30 July 2025.

<sup>32</sup>ED Shapiro and S Reifler, 'Forensic DNA Analysis and the United States Government' (1996) 36(1) *Medicine, Science and the Law* 43 <https://doi.org/10.1177/002580249603600109> accessed 30 July 2025.

<sup>33</sup>European Commission, 'Legal Framework for EU Data Protection' [https://commission.europa.eu/law/law-topic/data-protection/legal-framework-eu-data-protection\\_en](https://commission.europa.eu/law/law-topic/data-protection/legal-framework-eu-data-protection_en) accessed 27 December 2025.

DNA records are either anonymized or pseudonymized to guard against their misuse. The EU model focuses on transparency, control and the subjective rights as the aspects of data governance.<sup>34</sup>

Based on these three jurisdictions, some fundamental lessons can be pointed out that India can take to formulate its own legislation concerning DNA profiling and databases. One, there should be an autonomous body to regulate the use of DNA that is independent of police/ direct government control to make it accountable, and conduct audit. This body must have professionals in science, laws, ethics and human rights. Second, the government of India will have to abide by the principle of proportionality by gathering and preserving DNA that relates to a severe offense or an undoubted interest of the general population. Serious crimes should not collect DNA to charge a person of a lesser offence or in daily civil cases unless justified by a very serious reason.<sup>35</sup>

Third, automatic deletion of DNA records of the persons who were acquitted or not charged should be provided and definite time limits on retaining DNA records should be given based on the results of the case.<sup>36</sup> Fourth, the country of India should enforce anonymization and data minimization, or only the information that is not superfluous is gathered and that which can identify a person is not done so unless it is absolutely mandatory during investigations. Fifth, the right to dispute any inappropriate retention of their DNA and to seek expungement or damages in case of misuse or improper disclosure should be granted to people. Finally, transparency is something that is absolutely necessary, people should be notified when their DNA is being gathered, what is its purpose of use, and how long will it be there. Public reporting should also occur to maintain the trust of the people.<sup>37</sup>

To sum up, the experiences of the UK, USA and the EU indicate that efficient application of the DNA technology is actually possible without contravening on the basic rights. These best practices must be used by India and draft a legal framework that can encourage scientific progress and promote justice without violating the dignity, privacy, or autonomy of its citizens.<sup>38</sup>

## **8. CHALLENGES AND POLICY GAPS**

---

<sup>34</sup> TJ Kasperbauer, 'Protecting Health Privacy Even When Privacy Is Lost' (2020) 30(3–4) *Kennedy Institute of Ethics Journal* 285 <https://www.jstor.org/stable/27197981> accessed 27 December 2025.

<sup>35</sup> Barbara Prainsack and Vincent Toom, 'The Prüm Regime: Situated Dis/Empowerment in Transnational DNA Profile Exchange' (2010) 50(6) *British Journal of Criminology* 1117 <https://www.jstor.org/stable/43610847> accessed 27 December 2025.

<sup>37</sup> Carole McCartney, Tim Wilson and Robin Williams, 'The National DNA Database: Balancing Crime Detection, Human Rights and Privacy' (2011) 75(5) *Journal of Criminal Law* 406 <https://papers.ssrn.com> accessed 27 December 2025.

<sup>38</sup> AO Amankwaa and C McCartney, 'The Effectiveness of the UK National DNA Database' (2019) 1 *Forensic Science International: Synergy* 45 <https://papers.ssrn.com/> accessed 28 December 2025

India has a long way to go to implement the DNA Technology (Use and Application) Regulation Bill, 2019, with both challenges and policy gaps being noted in this regard. Lack of proper infrastructure and qualified workforce is one of the greatest impediments. At present, India does not possess sufficient well equipped forensic laboratories and trained man power capable of handling, analysing and processing DNA samples without any trouble. With the few resources available, there is already a backlog of forensic cases thus even further delaying the justice process. The significant size that national DNA databanks would necessitate is not technologically or logistically ready in many of the state facilities, and posing an urgent issue in terms of investing and training in this field.<sup>39</sup>

The other big problem lies in the vagueness concerning the clauses over civil use of DNA technology. The Bill gives the scope to utilize DNA profiling in civil cases that range to paternity issues, organ transplantation verification, and immigration. Nevertheless, the period during which such civil DNA records must be maintained and how these should be kept disassociated with any criminal-related repositories remain unidentified at the moment. This ambiguity creates the issue of potential abuse or over-regulation of genetic information gathering above that which is required, especially considering that there are no specific indices or evident deletion protection mechanisms of civil cases in the brought forth DNA databanks. People that have been engaged in civil disputes might find accidental implementation of the same level of surveillance or exposure to danger as the people on criminal investigations.

Other gaps should be oversight and accountability. Although there is a proposal of formation of a DNA Regulatory Board, as per the Bill, it grants the very wide powers to this body drafting regulations, overseeing laboratories itself, and interfering even with the regular privacy regulations. However, strong mechanisms of checks and review have not been evident in them. In contrast, to establish a separate data ethics authority or surveillance committee, as other states have already done, the proposed Indian system might enable a lot of discretion and lack of transparency which would most probably increase the likelihood of an error or abuse and the difficulty to remedy it.

To add to these problems, the DNA Bill is not aligned with the Data Protection Bill that was recently passed into law and now known as the Digital Personal Data Protection Act (DPDP Act), 2023.<sup>40</sup> The provisions of the DNA Bill which entail collection and storage of very sensitive biometric and genetic data are outdated and precede the well-rounded privacy protection and processes that the new data

---

<sup>39</sup>SCC Online, 'Challenges and Concerns in Admission of DNA Evidence in India' <https://www.sconline.com/blog/post/2022/04/06/challenges-and-concerns-in-admission-of-dna-evidence-in-india/> accessed 28 December 2025.

<sup>40</sup> *The Indian Express*, 'Explained: What Is the DNA Bill?' <https://indianexpress.com/article/explained/what-is-the-dna-bill-8857810/> accessed 29 December 2025.

protection regime has enacted. As a result, there is a risk of subjecting DNA data to levels of security and consent that are not optimal, or the procedures included in the DPDP Act may be bypassed. This state of disharmonizing renders individuals defenceless and annihilates the purpose of privacy privileges that were instituted in the law not that long ago.

Finally, a concomitant regulatory war between the authorities may take place. The Bill authorizes the DNA Regulatory Board to make sure that all issues relating to DNA profiling are regulated, but the DPDP Act creates an entirely different Data Protection Authority having a full mandate to regulate the processing of any sensitive personal information, including genetic information. The divisions of jurisdiction, or the inappropriate application of norms without an explicit agreement on which authority is in the first instance, how the liaisons between the two authorities will take place, may also be raised. This misconception could create loopholes and even shut down crucial processes and make the correct execution of the safeguards highly challenging.

## **9. RECOMMENDATIONS AND WAY FORWARD**

In India, the DNA technology (use and application) regulation bill is an important step toward upgrading forensic work and assisting the criminal justice system. Yet, some key amendments are advisable to make it more protective of the rights of individuals and at the same time improve the delivery of justice.

First, the Bill must find a close consideration to serious crimes only. This implies that the emphasis of the DNA profiling and databasing will have to be directed at crimes that attract more significant punishment like crimes that attract a sentence of more than seven years or life imprisonment.<sup>41</sup> Such a limitation to the application of the Bill can further assist in avoiding undue interference with the privacy of persons engaged in offenses of lesser degree or civil actions and limit the chances of possible abuse and over-application.<sup>42</sup>

Secondly, the Bill has to include more robust consent procedures<sup>43</sup>. This contains a requirement that the consent to collect a DNA sample must be informed, voluntary, and documented, preferably, in front of a magistrate, so that the individual is thoroughly aware of how their DNA will be utilized.<sup>44</sup> The

---

<sup>41</sup> P Das, 'Does Having a Universal DNA Database Prevent Crimes or Does It Prevent Justice?' (2023) *SSRN Electronic Journal* <https://doi.org/10.2139/ssrn.4322204> accessed 29 December 2025.

<sup>42</sup> D Uberoi, 'The Advent of Forensic DNA Databases: It's Time to Agree on Limits' (2023) *SSRN Electronic Journal* <https://doi.org/10.2139/ssrn.4666769> accessed 29 December 2025.

<sup>43</sup> AO Amankwaa, 'Trends in Forensic DNA Databases: Transnational Exchange, Data Protection and Privacy' (2019) 30(1) *Global Bioethics* 22 <https://doi.org/10.1080/11287462.2019.1578467> accessed 29 December 2025.

<sup>44</sup> A Zaretsky, 'DNA Collection in Immigration Custody and the Threat of Genetic Surveillance' (2021) 73(4) *Stanford Law Review* 807 <https://www.jstor.org/stable/27168416> accessed 29 December 2025.

Bill presently permits the magistrate to disregard consent in vague discretion that needs to be restricted by clear instructions and restrictions to prevent compulsion of individuals and defence of privacy right.<sup>45</sup>

Third, effective legal stipulation must be provided on how long the DNA profiles can be retained and what specific purposes they can serve. The permanent storage of DNA data, particularly of non-convicts or of convicts whose arrest is followed by acquittal, is against constitutional rights to privacy. The foreseeability of retention periods with a requirement to delete them upon case closure or acquittal will balance law enforcement requirements with personal rights.

Fourth, there is a significant need to establish independent and transparent commission to regulate DNA data processing, DNA labs, and access by law enforcers. This body must be independent of political oversight and impose accountability and provide ethical standards are observed. At the moment, the Bill gives a lot of powers to a Regulatory Board which lacks any checks and or has representation to the population, and thus risks concentration of power.<sup>46</sup>

Fifth, the Bill should be aligned with more extensive data protection legislation like Personal Data Protection framework in India. Since genetic information is a highly sensitive personal information, such intersection of genetic regulation and the national data privacy regime would ensure high protection, compensation of any complaints and harmonization with the constitutional requirements.<sup>47</sup>

Lastly, the collection of DNA in civil litigations or in cases that are not associated with crimes against humanity should be required to be approved by the courts. Unlike the criminal investigation where the concept of consent has got outs, the civil cases have to be required to undergo court supervision in order to compel a person to give DNA samples, hence not exposing individuals to arbitrary and exploitative applications of the technology. Therefore, the suggestions to the Bill on the DNA Technology will uphold the constitutional right of privacy, against self-incrimination and establish a forensic system that will be prepared to deliver justice timely and fairly. The Bill must have an element of transparency, being reasonable and the preservation of civil liberties as India opens up to modern DNA technologies.

---

<sup>45</sup> D Padmanabhan, 'DNA Technology and Civil Liberties: Re-Examining Consent, Retention and Oversight in India's DNA Bill' (2022) *SSRN Electronic Journal* accessed 29 December 2025.

<sup>46</sup> Erin Murphy, 'Forensic DNA Databases: Balancing Security, Privacy, and Equality' in M Killmister and I Kerr (eds), *Genetic Privacy and the Criminal Law* (Oxford University Press 2018) 45.

<sup>47</sup> N Grahanna and SN Nandini, 'DNA Fingerprinting and Its Implications on Indian Criminal Justice: A Constitutional Analysis' (2025) 3(2) *International Journal of Law, Ethics and Society* 145.

## **10. CONCLUSION**

To conclude, DNA technology is highly advantageous in improving justice and personal identifications but has serious legal and ethical problems. The main findings are that criminal justice can play a major role of benefiting and civil conflicts can be resolved through DNA profiling but that the current regulatory framework is poor and may cause infringements of privacy and abuse in India. The proposed DNA Technology Bill will fill some of these gaps although it will require a much deeper revision to ensure that it does not infringe on the rights of the constitution, specifically the right to privacy and fair trial.

It is vital to regulate DNA on a rights-based approach. This means that the collection, storage and use of the DNA data must be covered by laws that respect the individual freedoms and dignity. Informed consent, restricted application of genetic data, stringent time bound retention of data, and independent checking authorities are important guards against malpractice. Lacking such safeguards, one runs the risk of ending up with DNA databases abused through discrimination, unauthorized surveillance or wrongful inclusion.

Meanwhile, India also has to strike a balance between the embrace of modern technology and the democratic accountability. Clear guidelines on access and purpose, transparency in the processing of the data regarding DNA, and redress would be critical. Aligning with more general data protection laws will also enhance confidence and legal certainty in DNA-specific law. Thus, a considerate and safeguarding framework to the rights will make sure that the use of DNA technology is left to serve the societal needs and justice and protection of the rights. This is the balancing act that will be important to India as it embarks further to embrace the DNA innovations in a just, ethical and democratic way.

## **JUVENILE TRIALS: IMPROVING LEGAL, SOCIAL AND MENTAL HEALTH IN JUVENILE JUSTICE**

Vijay Kumar Verma\*  
Priyanka Bhati\*\*

---

### **ABSTRACT**

This paper presents a detailed analysis of the juvenile justice system, focusing on its historical evolution, current developments and future reform measures. Initially established in the spirit of reform and simplicity, the system has become punitive over time. It studies problems such as over-criminalization, racial and socio-economic disadvantage, lack of mental health services and cultural education. It emphasizes restorative justice, community-based interventions and property protection. Through policy analysis and empirical evidence, this research emphasizes the need to make the juvenile justice system humanistic and scope-enhancing.

***Keywords-** Juvenile Justice Reform, Rehabilitation, Juvenile Delinquency, Mental Health, Restorative Justice, Legal Policy, Child Rights*

### **2. INTRODUCTION TO JUVENILE JUSTICE**

In the present society, a punitive approach is adopted towards juveniles, whereas they need more correctional help. Juveniles, especially the poor and the underprivileged, are prone to harsh punishments due to their lack of mental immunity and socio-economic disability. The purpose of establishing the first juvenile court in 1899 was to ensure fairness, but over time the system became more dominant and punitive. Today the situation is that juvenile courts are promoting crime rather than reform. Basically it is necessary that we revive the basic spirit of this system, review and develop a justice system that maintains some balance.

---

\* Research Scholar, Teerthanker Mahaveer college of Law & Legal Studies, Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India

\*\* Assistant Professor, HIMT Group of Institutions, Greater Noida, Uttar Pradesh, India

### **3. HISTORICAL THEORY OF JUVENILE JUSTICE**

In the late 1800s, juvenile games were considered to be correctable and "juvenile courts" were established, whose purpose was not to punish, but to take care of the children and make decisions. Decisions were taken keeping in mind the social and family background. But after 1980, juvenile justice courts began to be charged with serious offenses and special protections were reduced. The juvenile justice system is now viewed as punishing, just like adult play, eroding the original reformatory approach.

### **4. CURRENT STATUS AND CHALLENGES OF THE JUVENILE JUSTICE SYSTEM**

The juvenile justice system and its associated clergy have changed little in the past two generations. Today, children are often relegated to the status of their parents' property and have limited legal rights. Rights that were fought for years - such as independent representation - many now feel are just part of the system's expansion. Most lawyers and advocates learn from low salaries and heavy-handed sharks, which slows down the process. Although the use of diversion programs has increased, their friendships have been limited. Many juveniles accept probation or other bondage to avoid serious pay that mars their records. Courts continue to operate from outdated, unfunded and laptop-from-the-supermarket bail bonds, which are considered a matter of social security rather than legal reform.

In contrast to alphabet-based approaches around the world, there is a renewed focus on juvenile justice reform. Nevertheless, many of the juvenile courts interviewed (Gebo, 2002) are often perceived as "too naturalistic", "informal" or "part of the problem", calling their image and friendliness into question. This perception stems from the ideological nature of the court's objectives, leading to mistrust, especially in minority communities (DN, 2008).

In addition, the juvenile court does not make decisions alone - police, prosecutors and other assistants also intervene in the process, limiting the court's role. Research has shown that factors such as ethnic identity, socio-economic status and labelling affect the juvenile justice process and recidivism rates. Most studies focus only on the process within the court, while social factors outside the court have a profound impact on the future of juvenile justice.

**Contemporary Challenges of Juvenile Courts:** Need for Reform Today, juvenile courts are facing many complex and multi-faceted narratives. The original purpose of the juvenile justice system was to focus on rehabilitation, social integration and holistic development, but at present the system seems to be deviating from its original purpose. The courts are now more inclined towards fundamental tendencies of harsh punishments, where the spirit of decency has been replaced by punitive tendencies. In many cases it has been observed that in criminal courts adult lawyers are treated as serious criminals, thereby violating their rights and power. This is contrary to the original spirit of the ancient Juvenile Justice Act, which claims that prison should not only be a punishment but also a hope for reform. At the same time, the impressive historical structure, structure, data collection and analysis, case management system, actors in the role of social court in juvenile courts are being ignored. The juvenile officers and related researchers are not getting contemporary information and training on juvenile psychology, short-term and community based. This article argues that there is still time to reorient juvenile courts toward their original purpose. This requires a comprehensive, multifaceted, and project-based reform that includes: **Management and structural audit of juvenile courts**

1. Training programs for philosophers, judges, and teachers
2. Expanding the community-based definition of justice
3. Juvenile participatory justice processes
4. Establishment of a monitoring and assessment system

If these reforms are implemented ethically, juvenile courts can once again become compassionate, egalitarian, and socially regenerative institutions.

## **5. JUVENILE CRIME STATISTICS AND TRENDS**

According to a 2013 report by the Office of Juvenile Justice and Delinquency Prevention, delinquency rates have declined by 48% over the past decade, particularly in cases of violent crime. However, nonviolent crimes such as property theft, dairy vendor cases and analysis are still at a high level. School, hospital and family services have proven to be more effective than crime prevention courts.

Many serious cases are still sent to adult courts, and statistics on noncriminal behavior are limited. Recent research has focused on court-designed models and the risk of major but limited jurisdiction

due to the limited jurisdiction of the court. From statutory certification, the active role of the police and noncriminal solutions to some crimes are positive signs.

## **6. ROLE OF REHABILITATION IN JUVENILE JUSTICE**

In contrast to alphabet-based approaches around the world, there is a renewed focus on juvenile justice reform. Nevertheless, juvenile courts face many challenges (Gebo, 2002). They are often perceived as "too natural", "informal" or "part of the problem", calling into question their image and friendliness. This perception stems from the ideological nature of the court's objectives, leading to mistrust, especially in minority communities (DN, 2008).

Furthermore, the juvenile court does not make decisions alone—the police, prosecutors and other facilitators also intervene in the process, limiting the court's role. Research has shown that factors such as ethnic identity, socio-economic status and labeling affect the juvenile justice process and recidivism rates. Most studies focus only on the process within the court, while social factors outside the court deeply influence the future of juvenile delinquency.

## **7. THERAPEUTIC APPROACH TO JUVENILE DELINQUENCY**

The juvenile justice system should adopt a therapeutic and developmental approach towards all juveniles, not a punitive one. Children seen as such need services, guidance and support to become responsible citizens in society.

### **Key Points:**

- Understanding instead of blame: Instead of tags like “guilty” or “innocent”, it is claimed that the limitations of life behavior are linked to cultural and mental development (Gebo, 2002).
- Access to services: Already access to professional professionals’ support services reduces the rate. But the main challenge is how to make this assessment high quality and qualitative (Slobogin and Fondacaro, 2009).
- Respect and rights: Children should be treated with respect and humanity while giving them legal and social identity.

## **8. NEW YORK MODEL AND ARIZONA REFORM**

**“Raise the Age” Policy:** is an important juvenile justice reform that aims to ensure that juveniles under the age of 18 are placed in the adult criminal justice system instead of the juvenile justice system. It has focused on psychologists, scientists and social scientists of believers, presenting them with a more human and statistical process.

**Establishment of an Orthodox "Youth Department":** An important and revolutionary step under the "age strengthening" policy was the establishment of the "Youth Department of the Criminal Court", especially in states like New York. This department is a special benchmark platform for hearing juvenile cases, which aims to adopt dialogue processes as part of the segments, through-groups and benchmarks of the juvenile justice system.

Juvenile Justice Reform in Arizona: Arizona has undergone significant reforms in the juvenile justice system in recent years, focusing on areas such as orderly, alternative justice, community-based interventions and records issues. It is said to be one of the few major US states that adopt a therapeutic and inclusive approach rather than punishments starting with juvenile delinquency.

## **9. COMMUNITY-BASED ALTERNATIVES**

An approach to the juvenile justice system is one that focuses on the improvement of the student's friend circle in society through counseling, education, and social services instead of punishment. This ideology focuses on reform and reintegration rather than punishment.

### **Major community-based alternatives:**

#### **1. Counseling and psychological services:**

- a. Individual, family, and group counseling.
- b. Assistance with de-addiction medication.

#### **2. Vocational and vocational training:**

- a. Re-entry of juveniles into school.
- b. Developmental skills programs, such as computer, Saudi, Badhigiri, etc.

#### **3. School service:**

- a. The juvenile is sentenced to serve a certain number of hours for the society, without being convicted.
- b. Example: cleaning public restaurants, variety, etc.

**4. Family-based interventions:**

- a. Training parents on how to guide their children.
- b. Solution to issues such as domestic violence, neglect, etc.

**5. Non-Residential Day Placement Centers:**

- a. Juveniles remain under supervision throughout the day and return home in the evening.
- b. Here they are given education, counseling and other services.

**6. Early Care and Guidance Programmes:**

- a. Assistance in grocery shopping after release from correctional home.
- b. Guidance by seniors.

**7. Girls in Schools:**

- a. Dialogue between crime and victims is established by finding solutions.
- b. A part of restorative justice.

**Advantages of Community-Based Alternatives:**

1. Juveniles remain in touch with society.
2. Chances of recidivism are less.
3. Mental and social development is promoted.
4. Prisons are less crowded.
5. Justice system is humane.

**10. DEVIATIONS FROM THE ORIGINAL PURPOSE**

The original concept of the juvenile justice system was to free juveniles from the stigma of the judicial process and conviction and give them a chance to live a life of their own.

- The attempt to not make juvenile court records public was made for this purpose.
- Its original principle was that juveniles be viewed and understood in different ways.

But in practice many reservations have been made, such as: removal of records in different courts, and the status of justice is different.

- The court process has now come under public scrutiny, causing lawyers to face legal challenges like a movie.

Harsh incidents of the courts

Where previously the purpose of the courts was to solo the fall, now their job is to separate them from solo life.

- Ownership of belongings is being limited and they are being sent to prison-like books.

Not fixed but harsh and limited punishments have now become common.

- Courts have given individual figures instead of applying strict procedural safeguards, thereby allocating courts and reducing the capacity of the strictest.

Documentation reform in the juvenile justice system is a complex and repository. Overcrowding in correctional facilities, limited resources and ineffective franchise programs adversely affect the rights and future of inmates. Lack of resources and overcrowding often lead to goods being sent out of state or to private goods, thereby failing the process of supervision and reform.

Reform efforts are ongoing in few states and where reform has taken place, there is a lack of prestige. Research often focuses on evaluation, not a thorough analysis of the performance of management concrete and local direction. New technologies are now stock of data-based assessments that can consider the consent and friendship of friends-lovers.

## **11. INCORPORATION OF THE ARCHAIC**

Technological innovations have deeply influenced courts around the world. Judiciary processes are now conducted virtually through webcams, laptops and aggregations such as video conferencing. In many cases these changes have become permanent and are transforming the nature of the justice system.

The design and operation of courts no longer require only physical equipment, but also technological equipment and practice. Although there is a wide variety in the practices and practices of different courts, a common challenge is how to strike a balance between innovation and the spirit of justice.

A major concern is how to maintain the process, the public and the trust of the public as technological advances are made. Public trust in any court is eroded when systems and judges fail to differentiate between them.

## **12. ROLE OF MENTAL HEALTH AND JUVENILE JUSTICE**

There is a strong connection between juvenile delinquency and mental health, but the juvenile justice system has little attention to juvenile delinquency and mental health needs. A large number of juveniles suffer from juvenile mental illness, yet they do not receive regular screening or treatment services. Courts often pass punitive decisions ignoring their mental condition, thereby further aggravating the problem. Services for youth are fragmented and affected due to lack of coordination between education and justice. Only through multi-agency support and community partnerships can youth be effectively provided with the necessary mental health services.

1. **Assessment and Treatment:** The purpose of assessment in the juvenile justice system is to assess risk of reoffending, delinquency, and mental health status (Scott and Grisso, 1997). Although most states provide similar assessment systems, their terminology and quality vary. Risk assessments estimate the likelihood of recidivism, while support assessments identify areas in need of improvement. However, there has been limited research on the effective use of these assessments and their role in reoffending prevention (Gebo, 2002). Services should be prioritized based on the findings of the assessment. Assessment systems exist in many states, but standardization could be done to enhance their principles and theories. There is a need to encourage society to have the best risk assessment at the state and regional levels.
2. **Impact of Mental Health on Crime:** Mental health problems such as depression, anxiety and conduct disorder affect juvenile court participation. Individuals are several times more likely to be arrested for a crime (Stoddard Dare et al., 2011). Mental health services in court, perceptions of children and racial concerns also affect participation. Aspects related to attention and supervision are also often overlooked. Early identification of the patient and contact with services to correct the problem can reduce the time taken in the process and prevent prevention of treatment. Understanding the role of mental health in the judicial process can lead to effective policies.

## **13. PARENTAL INVOLVEMENT IN JUVENILE JUSTICE**

Parents of adolescents often experience severe confusion and guilt. They want to guide their children on the right path, but circumstances make them feel powerless and destructive (Abdullah, 2014). To overcome this situation, they need to reevaluate their parenting practices, not just their initiation.

Parenting style has a profound impact on behavior—strict and repressive approaches can promote antisocial tendencies, while positive, communicative, and supportive parenting styles can help improve and develop.

#### **14. CHILD RIGHTS AND INTERNATIONAL STANDARDS**

This section examines the child rights on which the structure and principles of the juvenile justice system are based. This forum reviews international treaties designed to protect children's rights. The Convention on the Rights of the Child is the most important international treaty. It is the most widely ratified and most comprehensive treaty regarding children's rights. Nevertheless, many other treaties and declarations have shaped and continue to shape the Convention to this day. It considers the history of their development, how they shape the treatment of children globally in terms of human rights, and the principles that States follow to uphold those rights. Article 40 of the Convention on the Rights of the Child prohibits the criminalization of children under the age of 12 and offers detailed proposals for the treatment of children in conflict with the law. When considering the principles and tenets of Article 40, it must first be established that it does not include any child. A child is defined as every person under the age of 18. General Comment 10 defines the right to protection from interference by law and defines anyone under the age of 18 as a child (Gurahu, 2016). Nevertheless, there is freedom in relation to the portfolio of upper and lower age limits. The Convention on the Rights of the Child argues against the criminalisation of children under 12 – a view echoed in General Comment 10, which allows for the implications for justice by setting a minimum age of 12, but the study suggests a higher age. Yet, unfortunately, interpretations of guilt below this ‘standard’ are very high. The reality is that different standards apply globally in terms of minimum age and protection of children. Serious concerns exist about the criminalisation and proposed criminalisation of children under 12, as well as the consequences of lowering the age limit for defining children as children. However, it is also clear that this standard alone is meant to reflect the treatment and protection of all disadvantaged children, especially in a global environment where this underdeveloped age group is still more prevalent than others.

## **15. THE ISSUE OF DEMOCRACY AND JUSTICE**

The confidentiality and privacy of juvenile records is a serious concern for those involved with the juvenile justice system. Psychological philosophical research plays a key role in differentiating between adult and juvenile offenders' propensity for crime. The juvenile court was designed as a holistic, proactive response to crime rather than a punitive response. This work led to the popular perception of the juvenile court as a compassionate office where compassionate judges maintained patience and made every effort possible to maintain peace and alleviate the poverty of children. The protection of juvenile offenders from identification was considered a key component. However, criticism of juvenile records has gained more attention based on advances in data collection technology, media indifference regarding juvenile crime, and a growing grassroots movement aimed at holding violent offenders accountable for their actions (Lapp, 2015). A former teenager in a New York juvenile detention center who was accused of killing a taxi driver could not understand why her juvenile record was not opened or sealed even after her temple service was over. It is noteworthy that the inscriptions on juvenile records played a significant role in the critique of the juvenile court more than a century ago. It is believed that the signatures, pupils and behavior of juveniles in the juvenile court "shall not be published." Presumably, this reluctance to make juvenile records public is rooted in the philosophy of the initial juvenile court rather than in its punishment.

## **CONCLUSION**

This article is a distinguished history of the juvenile court system in the US, and attempts to cover some of the arguments in favor and nomination of the court as it currently is, and the establishment of the juvenile court as an institution that is emerging. It briefly describes three different theories of juvenile courts, and focuses on contemporary reforms. This article is intended as a source of insight into the history and debates surrounding the juvenile courts, and also as a challenge to current views and preserved records of the juvenile court (Gebo, 2002). The independence and constitution of the juvenile court can be maintained where it has stood for more than eighty years. The films that the juvenile court was developed to display remain unexplored today, and are likely to remain so as long as lawbreaking youth exist. The intervention and limited provision in the establishment of the juvenile court, protecting juvenile rights and publicizing the society for the public deportation of retribution (S.S. Scott and Grisso, 1997). Throughout history, each objective has been strongly highlighted by

the juvenile court in the US and similar social welfare initiatives in other countries. The juvenile court has been an attempt to insulate the juvenile offender from state punishment and to provide the juvenile offender in the United States with rights already available under the adult criminal process. Unfortunately, the malaise is deep and the juvenile-means-of-justice-connected-divisions advocated by the juvenile court in the US every couple of years, and especially during the last 20 years, an experience of an attempt to remedy the failure of this noble institution during adolescence, has been exhausted. The basis for the establishment of the juvenile court, created by it, and the well-proven mechanisms that cater to such students are constituted on the one hand by the internal judges and other institutions of the juvenile court, and on the other hand, by lawyers, examination officers, social lawyers, school authorities and other courts.

#### **REFERENCES:**

1. C. Quinn, M. (2012). Introduction: Evolving Standards in Juvenile Justice from Gault to Graham and Beyond. [PDF]
2. C. Feld, B. (2007). Unrestricted Punishment: Juvenile Criminal Responsibility and LWOP Penalties. [PDF]
3. S. Scott, E. and Grisso, T. (1997). The Development of the Adolescent: A Developmental Theory on Juvenile Justice Reform. [PDF]
4. Gebo, E. (2002). Juvenile Justice Reform: A Tale of Two Adolescents. [PDF]
5. M. Blankley, K. and Caldwell Jimenez, A. (2019). Restorative Justice and Youth Offenders in Nebraska. [PDF]
6. N. Berlinger, E. (2014). Youth: Restorative Justice and Social Work Practice. [PDF]
7. Reilly, J. (2012). Risk and Documented Factors of Crime: Large-Scale Approaches Working with Youth. [PDF]
8. J. Castelo, B., & Zozula, C. (2016). Peer influence: Mechanisms and motivations. [PDF]
9. Yaa A. Nyarko, N., Vera Aikins, L., Akosua Afriyie Nyarko, N., Amankwah Aboagye, E., & Yaa A. Nyarko, N. (2019). Juvenile delinquency: Its causes and effects. [PDF]
10. Wood, K. (2014). Setting up our children's future: Restoring access schooling through justice-friendliness. [PDF]

11. T. Russell, S., Wood, S., & Domeier, S. (1998). G98-1366 Establishing teen mentors in your community. [PDF]
12. McKinney, K. (2014). All about mentorship: An analysis of the most impactful life interventions in a Colorado juvenile shelter program. [PDF]
13. Dien, C. (2008). Forcing our children to watch movies like movies: recording children like movies. [PDF]
14. Sander, H., Lilchild, B., & Smith, N. (2006). Christian and minority ethnic groups and youth crime. [PDF]
15. Flax, S. & Flax, S. (2012). Youth justice reform: redressing age discrimination against children? [PDF]
16. Fretti, H. (2017). Deficiencies identified by the Clinical Social Society in mental health services in the juvenile justice system. [PDF]
17. A Stoddard Dare, P., A Mallett, C., & Boitel, C. (2011). The relationship between mental health disorders and adolescents. [PDF]
18. Abdullah, Z. (2014). Parents' experience of overseeing diversion legislation by their partners. [PDF]
19. Anne Labbe, P. (2015). A Study of After School and College-Related Youth Startup Programs in the Marginalized Northeast. [PDF]
20. Pearl Spivack, L. (2015). Ageing Up: Legal Reform for the Juvenile Justice System. [PDF]
21. Mallett, C. and Julian, L. (2008). Youth Program Alternatives: Reducing the Incarceration of Minority Youth in Cleveland, Ohio. [PDF]
22. Benedetto Netz, M. (2011). A Distinct Background, a Uniform Code: Assessing the Architecture of Juvenile Court. [PDF]
23. Guruhoo, J. (2016). According to the Juvenile Justice Act, a critical measure of the principle of this principle is that detention should be finalized and justice instances should be for a short period of time, strict in law. [PDF]
24. Lapp, K. (2015). Data-Based Analysis of Crime. [PDF]

**VIRTUAL HARASSMENT BUT REAL HARM-A STUDY ON SEXUAL  
OFFENCES AGAINST WOMEN IN DIGITAL ENVIRONMENT AND  
NEED FOR LEGAL REFORMS IN INDIA**

B.Veena Nirudhiya \*

---

**ABSTRACT**

The internet and technology are playing a pivotal role in our daily lives, which possesses both negative and positive impacts. On one side, it provides empowerment, and on the other side, it supports the anonymity of the perpetrator, causing abuse of others. Particularly, women are subject to various offences online, like cyberstalking, morphing, revenge pornography, etc. These kinds of offences, though not physically disturbing in all circumstances but cause psychological and social consequences, necessitating the need for addressing digital violence and legal reforms. This study concentrates on the nature and impact of sexual offences against women in the digital environment in India by analysing the efficiency of existing legal frameworks in India, exploring lacunae in the legislative measures. Through Doctrinal research, the paper emphasises the necessity for technologically advanced legal reforms, protecting the vulnerable rights of the victims. It is concluded with actionable recommendations, and the paper is inclusive of a clear view on cyber sexual offences, evolving offences like virtual rape in cyberspaces, societal perception, and the efficiency of the existing legal framework.

**Keywords:** Cyber offences, women, harassment, virtual rape, victim-blaming

---

\* 2<sup>nd</sup> year LLM(IPR), Government Law College, Tiruchirappalli, Tamil Nadu, India

## **1. INTRODUCTION**

Sexual offences against women are increasing and changing their pace from conventional to unconventional forms rather than decreasing across the globe. In the modern era, the fact that has become undeniable is that the Internet is playing an irreplaceable part in our lives. It replaced everything, and we are even heading towards a conundrum of whether artificial intelligence and humanoids will replace us.

Along with the development of other positive factors, cyberspace is taking us towards the path of an unsafe and traumatic environment, resulting in a variety of crimes, where it has become even unnecessary to see an individual to make a person become prey for his/her sexual feelings in an unwelcoming manner. Instead of reaching positive social transformation, the offences are getting advanced, and unfortunately, the legislative measures are getting outdated. The former perception that women are always victims of sexual offences has changed negatively, as along with even men and children are also exposed to these events. Such offences taking place in digital media are called cybercrime.

Cybercrime is a wide term including all sorts of offences and illegal activities taking place in cyberspace. It includes financial fraud, scams, hacking, online harassment, virtual rape, sextortion, usage of deepfake technology for such illegal activities, and various other new issues stemming at present. Cyber offences against women are at the top of the graph as usual, increasing day by day, affecting the physical and mental health of women in India, which needs serious concern and public attention. In addition to these, cyber sexual offences have become prevalent where it is causing both economic and psychological impacts on women.

## **2. OBJECTIVES OF THE RESEARCH**

- a. To study the concept of cyber sexual offences and their types.
- b. To determine how such offences are affecting the victims psychologically, specifically women.
- c. To examine how the Indian Legal Landscape is countering and tackling the issues stemming from the cyber sexual offences.
- d. To evaluate the legal frameworks in India in this aspect and identify the lacunae in adequately addressing the problem.

### **3. CYBER SEXUAL CRIME AGAINST WOMEN**

“Cyber sexual crime against women” is a broader term that includes social, economic, and psychological impacts on women. There is also a widely unnoticed factor, digital illiteracy. There is still a gap in attaining basic digital knowledge, irrespective of age. But in some cases, even digital illiteracy has no room in case of cyber hacking and other unethical means in reaching one’s device. There are several forms of sexual disturbances towards women in online platforms. Some of the offences which quite often affect women on a large scale are as follows:

#### **(i) Cyber harassment**

In India, cyber harassment also includes sexual harassment of victims which includes physical contact and advances, making sexual remarks, and asking for sexual favours<sup>1</sup>. It is unfortunate to say that online harassment has become one of the common crimes, where more women are affected due to these kinds of offences. According to a study by the National Commission for Women, 54.8% of women have experienced cyber harassment<sup>2</sup>. It is also pertinent to note that several sexual harassment cases occurred, by way of befriending a woman on social media platforms, which led such a woman to meet and caused sexual disturbances to her in person.

In addition to this, cyber sexual harassment can never be considered an offence constrained within the boundaries of one particular woman; rather, it causes negative consequences to the whole society itself. As how it affects the life of the victim of conventional sexual harassment and rape, this also significantly causes emotional trauma, irrespective of the victim’s age. In the case of Sanjeev Mishra vs. Bank of Baroda<sup>3</sup> the Rajasthan High Court extended the definition of "workplace harassment" to encompass online abuse.

In the virtual workplace, however, addressing and reporting sexual harassment is difficult because most employees are unfamiliar with the digital/virtual working model, the victim finds it difficult to

---

<sup>1</sup>The Sexual Harassment of Women at Workplace (Prevention, Prohibition, and Redressal) Act 2013, Section 2(n).

<sup>2</sup> Nature-Wise Report of the Complaints Received by NCW in the Year 2021 (<https://newapps.nic.in/firmReportNature.aspx?Year=2021>)

<sup>3</sup> Sanjeev Mishra v. Bank of Baroda, S.B. Civil Writ Petition No. 150/2021.

gather evidence on the digital platform, and even after gathering evidence, the victim is hesitant to file a complaint about fear of the case involving family members, as the investigation will involve<sup>4</sup>.

Cyber sexual harassment can be seen on all platforms in various forms. Sending unwanted or inappropriate comments or remarks which is sexual, sending sexually explicit content, or non-consensual pornography, which involves the online distribution of sexually graphic photographs or videos without the consent of the individual in the images, which can also be called revenge porn<sup>5</sup>, but unfortunately, Indian laws do not recognise it in particular.

This concept of sexual harassment includes sextortion, which is a form of non-physical forms of coercion to extort sexual favours from the victim and refers to the wide category of sexual exploitation in which abuse of power also occurs, as well as to the category of sexual exploitation in which threatened release of sexual images or information is the means of coercion<sup>6</sup>.

Financial extortion is the driving factor behind most cases. Other than these, cyber sexual harassment also includes sexual blackmail, impersonating to harass or intimidate others, or making unwanted sexual invitations or advances to make an individual feel emotional distress.

### **(ii) Virtual sexual assault and rape**

Although this concept is new, has no standard definition, and has not entered India yet, it is not far away. Virtual rape can be understood by way of the legal philosophical theories<sup>7</sup>. In simple terms, it refers to the intentional sexual assault or manipulation that someone forces on an avatar within a virtual environment like the metaverse, where people prefer to remain anonymous.

Virtual rape is complex, containing several dimensional approaches which are mandatory to be known for a better understanding of this offence. It can be categorized under this purview when

- a. A human user virtually sexually assaults a wholly virtual character using an avatar or

---

<sup>4</sup> Dershi Sharma, SEXUAL HARASSMENT IN THE VIRTUAL WORKPLACE, (<https://law.dypvp.edu.in/plr/Publication/all-publication/Sexual-Harrasment-at-Work-Place-ver-2.pdf>), *Pimpri Law Review, Volume 1, Issue 1* (2022)

<sup>5</sup> Revenge porn - European Institute of Gender Equality, available at [https://eige.europa.eu/publications-resources/thesaurus/terms/1459?language\\_content\\_entity=en](https://eige.europa.eu/publications-resources/thesaurus/terms/1459?language_content_entity=en), last visited on July 28, 2025.

<sup>6</sup> Futch Anthony Inso, 'Sextortion' in Naga: Man nabbed for trying to blackmail girl, 14, Cebu Daily News (November 13, 2024), available at <https://cebudailynews.inquirer.net/605696/sextortion-in-naga-man-nabbed-for-trying-to-blackmail-girl-14>, last visited on July 29, 2025.

<sup>7</sup> Strikwerda, L., Present and future instances of virtual rape in light of three categories of legal philosophical theories on rape. /, Vol. 28, No. 4, 2014, p. 491-510, available at (<https://sci-hub.se/10.1007/s13347-014-0167-6>), last visited on July 29, 2025.

- b. A human user virtually sexually assaults a virtual avatar that is controlled by another human being, using their own avatar or
- c. A human user virtually sexually assaults a wholly virtual character using immersive technology or
- d. A human user in virtual space sexually assaults a virtual avatar controlled by another human while using immersive technology or
- e. Wholly virtual character virtually sexually assaults a virtual avatar controlled by a human user or
- f. Wholly virtual character that virtually sexually assaults an avatar that is controlled by a human user using immersive technology<sup>8</sup>.

The report can be made against these activities by the aggrieved person, but there are still effective measures to be taken to rectify and help the victim in facing and curbing the issue. It is pertinent to note that for addressing this issue, the conventional essential elements which help to determine whether an act constitutes an offence provide a lending hand to certain extent.

Actus reus and Mens rea are the essential requirements to be satisfied in holding a person responsible in the physical world, but there arises a question on holding a wholly virtual character responsible in above mentioned cases, and this shows the complexity of facing this issue. But if the issue is about rape and other such sexual assaults, consent plays a vital role either in reality or in virtual space<sup>9</sup>.

### **(iii) Deepfake technology**

A deepfake can be a video, photo or even an audio recording which has been manipulated with AI, but looks real. The underlying technology can replace faces, manipulate facial expressions, synthesise faces, and synthesise speech. Deepfakes can depict someone appearing to say or do something that they never said or did<sup>10</sup>. The creation of fake images or videos depicting an individual, mostly an influential person, doing or opining on some topic that never happened significantly damages the reputation of such individuals in society.

---

<sup>8</sup> John Danaher, *The law and ethics of virtual sexual assault*, (Cheltenham, UK: Edward Elgar Publishers, 2018) available at <https://philpapers.org/archive/DANTLA.pdf>, last visited on July 28, 2025.

<sup>9</sup> *Ibid.*

<sup>10</sup> Science and tech spotlights – Deepfakes, available at <https://www.gao.gov/assets/gao-20-379sp.pdf>, last visited on July 28, 2025

This includes spreading false or misleading information, falsely depicting as stated by the competent authority or an individual having skill or knowledge in that particular domain, causing political manipulation with the help of this technology, and then attracting cyber sexual offences having serious consequences, as this leads to non-consensual pornography and raises privacy-related concerns.

This leads to an invasion of an individual's privacy, where the right to privacy<sup>11</sup> is envisaged under Article 21 of the Constitution of India, which also impliedly includes unauthorised utilisation in any manner causing encroachment upon their autonomy.

Furthermore, this technology is often misused, where women politicians are also subjected to non-consensual AI deepfakes, using their images and videos for inappropriate purposes<sup>12</sup>. This phenomenon is becoming common in most Western countries. There are measures taken by the countries, and it is also alarming at the same time that these artificial intelligence tools for generating such images and videos are in an affordable position, and it is not far from reaching our country either. Women, irrespective of their position in society, are equally affected due to the inappropriate usage of deepfake technology.

Other than the offences as mentioned earlier, the common threats faced by women all over the world, especially in India, are also still causing emotional distress. They are,

#### **(iv) Cyberbullying**

It is bullying with the use of digital technologies. It can take place on social media, messaging platforms, gaming platforms, and mobile phones. It can be like spreading lies about or posting embarrassing photos or videos of someone on social media<sup>13</sup>. Cyberbullying is more prevalent on all social media platforms. Spreading hatred towards everyone and bullying has become more common without considering the mental consequences faced by the victim.

#### **(v) Cyberstalking**

---

<sup>11</sup> KS Puttaswamy v. Union of India, (2017) 10 SCC 1.

<sup>12</sup> AI-generated deepfakes targeting women politicians around the world, The Hindu, dated January 07, 2025, available at <https://www.thehindu.com/news/international/ai-generated-deepfakes-targeting-women-politicians-around-the-world/article69071192.ece>, last visited on July 29, 2025.

<sup>13</sup> "Cyberbullying: what is it and how to stop it"- available at <https://www.unicef.org/end-violence/how-to-stop-cyberbullying>, last visited on July 29, 2025.

Stalking is generally defined as an ongoing course of conduct in which a person behaviourally intrudes upon another's life in a manner perceived to be threatening. But in cyberspace, cyberstalking, in a broader sense, is 'the use of the internet to stalk another person'.

According to internet safety organisations, the important characteristics of cyberstalking include some malice, premeditation, repetition, distress, obsession, vendetta, or if it is threatening, harassing, distressing, lacks a legitimate purpose, persists despite warnings to stop, or is personally directed, which often leads to physical stalking<sup>14</sup>.

#### **4. VICTIM BLAMING- A PERCEPTION OF SOCIETY**

Firstly, it is an irrefutable fact that patriarchal society and thoughts are predominant in India and a major reason for silencing the voice of the affected women. It is unfortunate that even in developed countries and also developing countries like India, gender-based disparity and violence are still not eradicated; on the contrary, it is getting higher day by day. Even today, male and female children are treated in unequal ways by their family members, teaching only female children how to perform their social duties as a "girl".

In addition to this, when the victim tries to interact about her experience with reporting agencies, hurdles are made by their family members, which affects the victim as she never opens up to protect her family's reputation<sup>15</sup>. Most of the victims are not reporting the incidents they faced due to social stigma and pressure<sup>16</sup>. Secondly, it became difficult for everyone to live without the internet and technology. It is nearly impossible to lead a life without the above-mentioned, as all the updates are made only by way of technology. People are subjected to internet addiction or social networking addiction, as we are indeed guided and influenced by what is shown on the screens, causing internet-guided behaviour<sup>17</sup>.

---

<sup>14</sup> Spitzberg, Brian H.; Hoobler, Gregory (February 2002), Cyberstalking and the technologies of interpersonal terrorism, (New Media & Society, Copyright © 2002 SAGE Publications London, Thousand Oaks, CA and New Delhi Vol4(1):67–88 [1461–4448(200202)4:1;67–88;020812]), available at "[Cyberstalking and the technologies of interpersonal terrorism](#)" (PDF), last visited on July 31, 2025.

<sup>15</sup> D. Halder & K. Jaishankar, Cyber Gender Harassment and Secondary Victimization: A Comparative Analysis of US, UK and India, available at ([https://www.researchgate.net/publication/239799976\\_Cyber\\_Gender\\_Harassment\\_and\\_Secondary\\_Victimization\\_A\\_Comparative\\_Analysis\\_of\\_the\\_United\\_States\\_the\\_UK\\_and\\_India](https://www.researchgate.net/publication/239799976_Cyber_Gender_Harassment_and_Secondary_Victimization_A_Comparative_Analysis_of_the_United_States_the_UK_and_India)) last visited on July 28, 2025.

<sup>16</sup> Ms. Akanksha Pathak Mr. Prateek Tripathi, DIGITAL VICTIMIZATION OF WOMEN IN CYBERSPACE: AN ANALYSIS OF EFFECTIVENESS OF INDIAN CYBER LAWS, available at (<https://nluassam.ac.in/docs/Journals/NLUALR/Volume-7/Article%207.pdf>), last visited on July 29, 2025.

<sup>17</sup> *Ibid.*

On one hand, Cyber sexual harassment is causing such a negative influence on women, on the other hand, instead of giving a hand to help the victims, they are blamed for using social media and subjected to different aspects of the act of victim-blaming, which is commonly seen in all other sorts of women affected by offences in society.

In this digital era, social media is widely used for making connections, job searching, and professional networking, where avoiding modern technology can never be a solution to handle the situation. Rather than speaking only about what women can do from her side, it is the need of the hour to focus on eradicating these kinds of offences by tracing the perpetrators of these criminal offences. The usage of such platforms responsibly applies to both the victim and the perpetrator, irrespective of their gender.

Furthermore, Web surfing, online shopping, sexual addiction like online relationships, watching porn sites and playing computer games are known to be predominant internet addictive behaviours. It offers people the liberty to do what cannot be done in real life, which can be taken in both positive and negative aspects. Anonymity can be maintained and it makes it difficult for authorities to trace out the offender behind the screen. Due to easy and quick accessibility, availability and holding a significant position in every task of our lives, the internet has become inevitable and slowly engulfing our lives. This clearly shows that due to this unavailability, women are captured by the hands of perpetrators easily.

Thirdly, the influence of social media platforms is huge and causes negative implications. This increases inquisitiveness, which pushes us to keep an eye on everyone's life as well as to show what is happening in our lives, even though we are well aware of the violation of privacy by these social media platforms. It becomes easy for the perpetrators to trace out all the necessary details of the victim and can be used against her at any time.

As women are often blamed in most cases, due to victim blaming also, in fear, women often do not voice out their negative experiences. Due to this, perpetrators are fearless and victims are blamed, but it should be changed so that victims get support and perpetrators should know what they are doing and be punished.

## **5. LEGAL LANDSCAPE, LOOPHOLES AND LANDMARK CASES ADDRESSING CYBER CRIME**

Cybercrime is still considered a non-serious crime due to a lack of awareness in India. The Indian Government is taking steps to control and regulate the issues faced in cyberspace, but also, the laws introduced are also getting outdated. Major laws existing as a shield for fighting these issues are the Information Technology Act, 2000, Bharatiya Nyaya Sanhita 2023 which replaced the Indian Penal Code 1860, Indecent Representation of Women (Prohibition) Act, 1986 and several other Acts like Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013.

To effectively eradicate sexual offences against women in cyberspace, the proper implementation of these laws and the introduction of specific laws are the need of the hour. The laws and their effectiveness are given more focus so that quick and adequate attention will be given, and victims can get appropriate results.

**(i) The Information Technology Act, 2000:**

This Act is a milestone in addressing internet and technological problems but the demerit is that this Act is not sufficient in combating the present issue. This is more focused on dealing with e-commerce and financial institutions in general. But it is important for addressing the protection of women in cyberspace, attacks and challenges faced by them specifically and separately.

Indeed, provisions<sup>18</sup> focus on penalising the publishing and transmission of sexually explicit content, but specific lacuna about addressing particularly cyber sexual crime against women still exist due to generalising and constraining the issues only within the ambit of online sex abuse, morphing, pornography, and cyberstalking rather than speaking about the crime occurring due to advancement of technology and agony faced in consequence. For instance, sextortion cases are increasing<sup>19</sup>, causing danger for both male and female children and the concept of virtual rape is alarming in digital space<sup>20</sup>. Also, there are no effective measures about the removal of already surfaced images or videos of the victim. To protect women in India from such kinds of crimes, it is necessary to fill those lacunae.

But in case of holding intermediaries liable, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 hold social media platforms accountable and liable for

---

<sup>18</sup> The Information Technology Act, 2000, Sections 67, 67A, and 67B.

<sup>19</sup> Global Threat Assessment 2023 Assessing the scale and scope of child sexual exploitation and abuse online, to transform the response- WeProtect Global Alliance, available at <https://www.weprotect.org/global-threat-assessment-23/#full-report>, last visited on July 30, 2025.

<sup>20</sup> First case of virtual gang rape reported in Metaverse, investigation *underway*, The Indian Express, dated January 4, 2024 available at <https://indianexpress.com/article/technology/social/virtual-gang-rape-reported-in-metaverse-uk-9093462/>, last visited on July 30, 2025.

ensuring user safety by benefiting users on one hand and require a proper redressal mechanism from the side of the intermediaries.

Intermediaries must communicate their terms and conditions, including not allowing any content which is harmful, unlawful, obscene, or invasive of another's privacy, and removing any information violative of Indian law<sup>21</sup>. It is important to address the individual effects of women victims by way of specific legislation with more updates concerning technical advancement.

**(ii) Bharatiya Nyaya Sanhita, 2023 (then, Indian Penal Code, 1860)**

The Indian Penal Code was repealed and replaced by Bharatiya Nyaya Sanhita in 2023. In the former code, there are some glimpses of addressing cybercrime offences, but the sections do not particularly address the offences as mentioned earlier.

Some of the provisions stated about the sale of obscene materials<sup>22</sup>, voyeurism<sup>23</sup> and stalking<sup>24</sup> were interpreted accordingly for cybercrime offences. The first cyberstalking case was reported in the year 2001<sup>25</sup>, where Manish Kathuria was stalking Ritu Kohli, used obscene language and distributed her telephone number without her permission due to which she was subjected to obscene calls from various states of India and other foreign countries, she reported the case but due to the absence of particular section about this, he was registered under section 509 of Indian Penal Code speaking about outraging the modesty of women. As there is a lacuna in speaking about stalking on the Internet in both old law and new law, there are no proper proceedings against the perpetrators. Starting from this case, several cyber stalking, morphing<sup>26</sup>, and cyber defamation<sup>27</sup> had taken place but there is still a gap in addressing the problem and punishing the perpetrator, as the provisions in the previous code and new Act, there are generalised sections to cybercrime.

---

<sup>21</sup> Measures To Ensure Safety And Security Of Women And Children On Online Platforms- Press Information Bureau Government of India- Ministry of Women and Child Department (2022), available at <https://www.pib.gov.in/Pressreleaseshare.aspx?PRID=1808686>, last visited on July 28, 2025.

<sup>22</sup> The Indian Penal Code, 1860, Section 292, now Bharatiya Nyaya Sanhita, 2023, Section 294.

<sup>23</sup> The Indian Penal Code, 1860, Sections 354C, now Bharatiya Nyaya Sanhita, 2023, Section 77.

<sup>24</sup> The Indian Penal Code, 1860, Sections 354D, now Bharatiya Nyaya Sanhita, 2023, Section 78.

<sup>25</sup> Manish Kathuria v Ritu Kohli, 2001.

<sup>26</sup> Vinupriya suicide case, Times of India (Aug 3, 2016)- available at <https://timesofindia.indiatimes.com/city/chennai/only-1-6-of-cybercrime-victims-approach-police-for-help-survey/articleshow/53519299.cms>, last visited on July 30, 2025.

<sup>27</sup> SMC Pneumatics India Pvt. Ltd. Vs Jogesh Kwatra, CS(OS) No. 1279/2001 (Delhi High Court, 2001)

Even though cyber sexual assault cases, we have laws which are focussing only on an economic perspective. Furthermore, it is unfortunate that most of the cyber sexual offence cases are not being complained and reported compared to other offences<sup>28</sup>. The Penal laws are still in need of adequate development in combating several sexual offences. Apart from circumscribing women affecting issues only within the ambit of abuse and rape, various new kinds of offences have occurred and such abuse and rape are also getting converted from one medium and another. It is getting tedious for both law-making and law-enforcing authorities to control these offences.

**(iii) Indecent Representation of Women (Prohibition )Act, 1986**

The aim of the Indecent Representation of Women (Prohibition) Act of 1986 is to prohibit the publishing of obscene advertisements and the indecent representation of women. The Act was to be amended to be on par with the punishment prescribed in the Information and Technology Act and was made to be applied to digital media<sup>29</sup>. The Act have to be updated concerning modernisation and avoid conflict based on gender-specific morality with clear explanation about “obscenity”, with specific representation of women's victimisation through indecent portrayal.

**(iv) Digital Personal Data Protection Act, 2023**

This Act is established primarily to protect vast data due to digitalisation and can help to protect personal data from misuse due to the rapid evolution of technology and high cyber threats. For protecting the economic growth of India, this Act plays a vital role, but in the case of addressing cyber sexual crime against women, this Act has only a small part as this Act helps in personal data protection for upholding national security.

**(v) Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013.**

The Act was introduced after the landmark judgment- Vishaka and Ors v. State of Rajasthan and Ors<sup>30</sup> for addressing sexual harassment faced by women in their workplaces and providing for raising complaints and redressal.

---

<sup>28</sup> Nature-wise and State-wise number of cases registered during 2024 ([https://ncwapps.nic.in/firmComp\\_stat\\_Overview.aspx](https://ncwapps.nic.in/firmComp_stat_Overview.aspx)).

<sup>29</sup> *Ibid.*

<sup>30</sup> Vishaka and Ors v. State of Rajasthan and Ors, AIR 1997 SC 301.

Since there is no specific mention of cyber sexual offences in the Act, the noteworthy effort made by the Indian Judiciary in several judgments is the wide interpretation of the term “workplace”. From speaking about the theory of notional extension, covering the employer’s liability is not limited to the physical boundary of the “workplace”; it is further extended beyond, which can be construed within the purview of providing safety for working women in cyberspace. During the outbreak of the COVID-19 pandemic, conventional workplaces evolved, and there was an introduction of “work from home” culture. There were several issues faced by women within the ambit of cyber sexual harassment in virtual workplaces, also<sup>31</sup>.

Positively, the Act helped in countering the issue, which was proved in the case of *Jaya Kodate v. Rashtrasant Tukdoji Maharaj Nagpur University*<sup>32</sup>, it was decided that the term “workplace” is not restricted within the purview of the physical workplace alone, and by considering the legislative intent of the Parliament in introducing this Act, the definition of the term is wide and it also includes the cyber environment.

## **6. CONCLUSION AND RECOMMENDATIONS**

Our society is dynamic, and so is crime. The nature of laws should be constantly evolving forward. Particularly, sexual crime against women is significantly on the rise, and it is getting advanced and causing fear in women. Unfortunately, these types of offences are evolving negatively, affecting more women and extending their arms towards men and children. The transformation of crime is so quick that it needs more caution in protecting and preventing the victims. Technology has the power to influence the behaviour of an individual either positively or negatively. India is towards a futuristic pathway, where there are an enormous number of startup businesses and various other fields are in a boom; indeed, there is a major role to be played by technology. In the long run, every individual requires the development of various new skills to survive, where the goals can be reached with the help of technology in the present situation. But, if women are dragged down without proper addressing of these kinds of issues, it will lead to difficulty in reaching positive transformation in Indian society.

---

<sup>31</sup> *Supra note 5.*

<sup>32</sup> *Jaya Kodate v. Rashtrasant Tukdoji Maharaj Nagpur University*, Civil Writ Petition No. 150, Bombay High Court (2012).

Our law-making bodies are making enormous efforts in curbing the issues, but still, the major lacunae in most of our laws are that the laws are approaching more general rather than specific representations of individual issues. Instead of generalising the crime that occurred and fitting it in a particular section, there may be specific legislation addressing all kinds of cybercrime occurring in the country, specifically about cyber sexual offences in India, for effective transformation in a positive way. Unfortunately, the only practice which has not changed or transformed in our society is blaming the victim. People in our society should think from the perspective of the victim rather than stating what should have been done and not have been done.

Rather, we, the society, should support the victim when the problem is faced according to the advancement and development in society. Cyber sexual offences are indeed violating privacy, causing emotional distress and mental trauma. It may be fruitful when there is a proper redressal forum for cybercrime in India, as this has become a weapon in the hands of perpetrators in threatening women, people and the country as a whole. This will encourage the victims to report the injustice that occurred to them when the Government itself is giving its support to them. Apart from punishing those who are involved in such a crime, the welfare of the victim should also be considered. As the upcoming generations are growing along with technical advancement, teaching them about dignified usage of the internet, respecting everyone equally and not misusing the advantage of the advancement of technology plays a positive role in transforming society in a better way.

## **“CORPORATE SOCIAL RESPONSIBILITY (CSR) AND ITS IMPACT ON CORPORATE GOVERNANCE”**

Samay Jain\*  
CS(Dr.) Pallavi Baghel\*\*

---

### **ABSTRACT**

“Corporate Social Responsibility (CSR) has become a crucial aspect of modern business practices. This research examines the impact of CSR on corporate governance in India”. It explores how CSR initiatives influence governance practices and stakeholder engagement. The study focuses on analysing the current status of CSR implementation, comparing it to international standards, and identifying gaps in Indian laws and regulations. It investigates the implications of non-compliance with CSR guidelines and analyses landmark judicial responses related to CSR implementation. The research employs doctrinal legal methodology, relying on legal texts and judicial decisions as primary sources. The findings aim to provide valuable insights into CSR implementation in India and suggest necessary improvements for effective governance.

**Keywords:** Corporate Social Responsibility, India, Corporate Governance, Stakeholder Engagement, Judicial Responses, Non-Compliance.

---

\* Final year LLB candidate, Symbiosis Law School, Pune

\*\* Assistant Professor, Symbiosis Law School, Pune, Symbiosis International University

## **INTRODUCTION**

“Corporate Social Responsibility (CSR) has emerged as a crucial aspect of modern business practices. In today's globalized world companies are expected to go beyond mere profit-making and contribute positively to society and the environment.<sup>1</sup> CSR has become an integral part of corporate strategy with businesses recognizing the importance of sustainable development and stakeholder engagement.<sup>2</sup> The increasing attention given to CSR can be attributed to several factors including growing public awareness of social and environmental issues” heightened scrutiny from media and civil society organizations and the realization that responsible business practices can lead to long-term success and competitiveness.<sup>3</sup>

In the Indian context “CSR has gained significant momentum in recent years particularly after the enactment of the Companies Act 2013 which mandates certain companies to spend a portion of their profits on CSR activities.<sup>4</sup> This research aims to examine the impact of CSR initiatives on corporate governance practices and stakeholder engagement in India. It argues that CSR plays a vital role in shaping governance structures decision-making processes and the way companies interact with their stakeholders. By integrating CSR into their core business operations Indian companies can enhance transparency accountability and ethical behavior leading to better corporate governance and improved stakeholder relations”.

## **CORPORATE SOCIAL RESPONSIBILITY (CSR)**

### **A. Definition and scope of CSR**

“Corporate Social Responsibility (CSR) refers to the voluntary actions taken by companies to address social and environmental concerns while conducting their business operations.<sup>5</sup> It encompasses a wide range of activities that go beyond legal compliance and aim to contribute positively to society such as philanthropy community development environmental sustainability and ethical business

---

<sup>1</sup> “A Kolk 'The Social Responsibility of International Business: From Ethics and the Environment to CSR and Sustainable Development' (2016) 51 Journal of World Business 23. ”

<sup>2</sup> “R Panda and NM Modak 'Corporate Social Responsibility: Conceptual Framework and Strategies for Sustainable Development' in NM Modak (ed) Corporate Social Responsibility in India: Cases and Developments after the Legal Mandate (Springer 2016). ”

<sup>3</sup> “T Mahmood 'Corporate Social Responsibility: The New Corporate Mantra' (2019) 40 Vikalpa 287. ”

<sup>4</sup> “Debnath Chatterjee 'India Corporate Social Responsibility: An Analysis' (Pacific Business Review Vol 3 Issue 7 January 2011) 43. ”

<sup>5</sup> “P Holme and J Watts 'Corporate Social Responsibility: Making Good Business Sense' (World Business Council for Sustainable Development 2000) 8. ”

practices.<sup>6</sup> CSR is based on the premise that businesses have a responsibility towards their stakeholders including shareholders employees customers suppliers and the communities in which they operate.<sup>7</sup> The scope of CSR extends to various domains including labor practices human rights environmental protection anti-corruption measures and stakeholder engagement”.<sup>8</sup>

## **B. Evolution of CSR in India**

### *1. Historical context*

“The concept of CSR is not new to India with its roots dating back to ancient times”. Indian businesses have traditionally engaged in philanthropic activities such as building temples schools and hospitals as part of their social obligations.<sup>9</sup> During the colonial era prominent industrialists like Jamshetji Tata and G.D. Birla were known for their social welfare initiatives.<sup>10</sup> Post-independence the Indian government emphasized the role of businesses in nation-building and social development. The concept of "trusteeship" advocated by Mahatma Gandhi which urged businesses to act as trustees of societal wealth gained prominence.<sup>11</sup>

### *2. Mandatory CSR under the Companies Act 2013*

“A significant milestone in the evolution of CSR in India was the enactment of the Companies Act 2013. Section 135 of the Act mandates certain companies to spend at least 2% of their average net profits made during the three immediately preceding financial years on CSR activities.<sup>12</sup> The Act applies to companies with a net worth of INR 500 crore or more a turnover of INR 1000 crore or more or a net profit of INR 5 crore or more during any financial year.<sup>13</sup> The introduction of mandatory CSR spending has led to a significant increase in CSR activities and expenditure by Indian companies”.<sup>14</sup>

---

<sup>6</sup> “A Rasche M Morsing and J Moon (eds) Corporate Social Responsibility: Strategy Communication Governance (Cambridge University Press 2017). ”

<sup>7</sup> “A McWilliams and D Siegel 'Corporate Social Responsibility: A Theory of the Firm Perspective' (2001) 26 Academy of Management Review 117. ”

<sup>8</sup> “ISO 26000:2010 Guidance on Social Responsibility (International Organization for Standardization 2010). ”

<sup>9</sup> “Ramesh Kumar 'The Interface of Corporate Social Responsibility and Corporate Governance: The Indian Context' (2019) 9 Indian Journal of Corporate Governance 39. ”

<sup>10</sup> “SY Cheruvu and D Govind 'Corporate Social Responsibility: A Historical Perspective from India' (2017) 4 International Journal of Research in Social Sciences 473. ”

<sup>11</sup> “GD Sharma 'Corporate Social Responsibility in India: An Overview' (2009) 43 The International Lawyer 1515. ”

<sup>12</sup> “The Companies Act 2013 s 135. ”

<sup>13</sup> “The Companies (Corporate Social Responsibility Policy) Rules 2014. ”

<sup>14</sup> “KS Rana 'Corporate Social Responsibility: The Way Ahead' (The Economic Times 8 June 2017). ”

### **C. Key areas of CSR activities**

#### *1. “Environmental sustainability”*

“Environmental sustainability is a key focus area for CSR initiatives in India. Companies are increasingly investing in green technologies renewable energy waste management and water conservation projects to minimize their environmental footprint”.<sup>15</sup> For example Tata Power has set up wind and solar power projects across the country to promote clean energy.<sup>16</sup> ITC Limited has implemented a comprehensive water stewardship program which includes rainwater harvesting watershed development and water efficiency measures.<sup>17</sup>

#### *2. Social welfare and community development*

CSR activities in India also prioritize social welfare and community development initiatives. Companies engage in various projects aimed at poverty alleviation education healthcare skill development and women empowerment.<sup>18</sup> For instance Reliance Industries Limited has established the “Reliance Foundation” which focuses on rural transformation education health and disaster response.<sup>19</sup> Hindustan Unilever Limited runs the "Project Shakti" program which empowers rural women by providing them with entrepreneurial opportunities.<sup>20</sup>

#### *3. Ethical business practices*

Promoting ethical business practices is another important aspect of CSR in India. Companies are increasingly adopting codes of conduct anti-corruption policies and transparent reporting mechanisms to ensure integrity and accountability in their operations.<sup>21</sup> The Tata Group known for its strong ethical values has a comprehensive “Tata Code of Conduct that guides the behavior of its employees

---

<sup>15</sup> “A Saxena 'Corporate Social Responsibility for Environmental Protection and Conservation: A Review of Initiatives by Indian Companies' (2019) 9 International Journal of Business and Social Science 1. ”

<sup>16</sup> “Tata Power 'Sustainability' accessed 20 April 2023. ”

<sup>17</sup> “ITC Limited 'Sustainability Initiatives' accessed 20 April 2023. ”

<sup>18</sup> “P Gupta and S Sharma 'Corporate Social Responsibility in India: Trends Issues and Strategies' (2017) 3 International Journal of Science and Research 1655. ”

<sup>19</sup> “Reliance Foundation 'Focus Areas' accessed 20 April 2023. ”

<sup>20</sup> “Hindustan Unilever Limited 'Sustainable Living' accessed 20 April 2023. ”

<sup>21</sup> “S Bhaskar 'Corporate Governance and Ethics in India' (2016) 1 International Journal of Law and Management 122. ”

and business partners.<sup>22</sup> Infosys a leading IT company has established a robust whistleblower policy and an ethical governance framework to maintain high standards of corporate governance”.<sup>23</sup>

## **CORPORATE GOVERNANCE IN INDIA**

### **A. “Definition and principles of corporate governance”**

“Corporate governance refers to the system of rules practices and processes by which a company is directed and controlled.<sup>24</sup> It involves balancing the interests of various stakeholders such as shareholders management employees customers suppliers and the community at large.<sup>25</sup> The principles of corporate governance include transparency accountability responsibility and fairness.<sup>26</sup> Effective corporate governance ensures that companies are managed in a manner that protects the rights of shareholders promotes ethical decision-making and enhances long-term value creation”.<sup>27</sup>

### **B. Regulatory framework for corporate governance in India**

#### *1. “The Companies Act 2013”*

“The Companies Act 2013 is the primary legislation governing corporate governance in India. It lays down various provisions related to the incorporation management and administration of companies.<sup>28</sup> The Act emphasizes the roles and responsibilities of directors the composition and functioning of board committees and the disclosure and reporting requirements for companies”.<sup>29</sup> It also introduced provisions related to independent directors women directors and CSR aimed at strengthening corporate governance practices in India.<sup>30</sup>

#### *2. SEBI guidelines and listing agreements*

“The Securities and Exchange Board of India (SEBI) is the regulatory body responsible for supervising and regulating the Indian securities market. SEBI has issued various guidelines and regulations to enhance corporate governance standards for listed companies.<sup>31</sup> The SEBI (Listing

---

<sup>22</sup> “Tata Group 'Tata Code of Conduct' accessed 20 April 2023. ”

<sup>23</sup> “Infosys 'Corporate Governance' accessed 20 April 2023. ”

<sup>24</sup> “The Institute of Company Secretaries of India 'Corporate Governance' accessed 20 April 2023. ”

<sup>25</sup> “V Balachandran and R Chandrasekaran (eds) Corporate Governance Ethics and Social Responsibility (PHI Learning Pvt Ltd 2011). ”

<sup>26</sup> “B Tricker Corporate Governance: Principles Policies and Practices (3rd edn Oxford University Press 2015).”

<sup>27</sup> “PN Sinha 'Corporate Governance and Value Creation' (2014) 4 The IUP Journal of Corporate Governance 7.”

<sup>28</sup> “DK Jain Company Law I (Ascent Publications 2018). ”

<sup>29</sup> “The Companies Act 2013. ”

<sup>30</sup> “K Vaidyanathan and D Prasad Company Law Ready Reckoner (Wolters Kluwer India Pvt Ltd 2017). ”

<sup>31</sup> “VK Pandey 'Corporate Governance in India: Regulatory Reforms and Challenges' (2018) 7 International Journal of

Obligations and Disclosure Requirements) Regulations 2015 prescribe comprehensive governance norms for listed entities including board composition related party transactions and disclosure obligations.<sup>32</sup> Listed companies are required to enter into listing agreements with stock exchanges which mandate compliance with SEBI's corporate governance requirements".<sup>33</sup>

### **C. Role of the board of directors in corporate governance**

"The board of directors plays a pivotal role in ensuring effective corporate governance. The board is responsible for setting the strategic direction of the company overseeing management performance and protecting the interests of stakeholders.<sup>34</sup> The Companies Act 2013 and SEBI regulations specify the duties and responsibilities of directors including acting in good faith exercising reasonable care and diligence and avoiding conflicts of interest.<sup>35</sup> The board is also required to constitute various committees such as the audit committee nomination and remuneration committee and stakeholders' relationship committee to ensure proper oversight and governance".<sup>36</sup>

### **D. "Importance of transparency and disclosure"**

"Transparency and disclosure are fundamental pillars of good corporate governance. Companies are required to disclose material information to their stakeholders in a timely and accurate manner.<sup>37</sup> The Companies Act 2013 and SEBI regulations mandate various disclosures including financial statements board reports related party transactions and shareholding patterns".<sup>38</sup> Transparency helps build trust among stakeholders reduces information asymmetry and enables informed decision-making.<sup>39</sup> It also facilitates market discipline and allows stakeholders to "hold companies accountable for their actions".<sup>40</sup>

---

Business and Management Invention 26. "

<sup>32</sup> "SEBI (Listing Obligations and Disclosure Requirements) Regulations 2015. "

<sup>33</sup> "R Kalra and A Rai 'Role of SEBI in Corporate Governance' (2015) 7 International Journal of Scientific & Engineering Research 899. "

<sup>34</sup> "RM Hanson 'The Role of the Board of Directors in Corporate Governance' (2014) 29 Corporate Governance Advisor 1. "

<sup>35</sup> "The Companies Act 2013 ss 166 and 149. "

<sup>36</sup> "SEBI (Listing Obligations and Disclosure Requirements) Regulations 2015 reg 18 19 and 20. "

<sup>37</sup> "L Nohria and R Khurana (eds) Handbook of Leadership Theory and Practice: A Harvard Business School Centennial Colloquium (Harvard Business Press 2010). "

<sup>38</sup> "The Companies Act 2013 ss 129 134 188 and 92. "

<sup>39</sup> "A Cadbury Report of the Committee on the Financial Aspects of Corporate Governance (The Committee on the Financial Aspects of Corporate Governance and Gee and Co Ltd 1992). "

<sup>40</sup> "VM Govindarajan and VK Govindarajan 'Market Discipline and Corporate Governance' (2018) 52 Economic & Political Weekly 67. "

## **RELATIONSHIP BETWEEN CSR AND CORPORATE GOVERNANCE**

### **A. CSR as a component of good corporate governance**

CSR is increasingly recognized as an integral component of good corporate governance. Incorporating CSR into corporate governance frameworks ensures that companies consider the broader societal and environmental impacts of their decisions.<sup>41</sup> CSR helps align business objectives with stakeholder expectations and promotes sustainable value creation.<sup>42</sup> By integrating CSR into governance structures companies “demonstrate their commitment to responsible business practices and enhance their reputation and credibility”.<sup>43</sup>

### **B. Impact of CSR on board decision-making and oversight**

CSR considerations “have a significant impact on board decision-making” and oversight. Boards are expected to consider the interests of various stakeholders while making strategic decisions.<sup>44</sup> CSR-related risks and opportunities are becoming important factors in board deliberations. Boards are responsible for setting the tone at the top and ensuring that CSR is embedded in the company's culture and operations.<sup>45</sup> They also play a crucial role in overseeing the implementation of CSR policies monitoring CSR performance and ensuring adequate resources are allocated to CSR initiatives.<sup>46</sup>

### **C. CSR and stakeholder engagement**

#### *1. Increased focus on stakeholder interests*

CSR emphasizes the “importance of considering and balancing the interests of various stakeholders beyond just shareholders.”<sup>47</sup> Companies are recognizing the need to engage with their stakeholders understand their concerns and address their expectations.<sup>48</sup> Stakeholder engagement helps companies identify material issues assess their impacts and develop effective CSR strategies.<sup>49</sup> By focusing on

---

<sup>41</sup> “M Arora and D Srivastava 'Corporate Social Responsibility and Corporate Governance in India: A Review' (2019) 7 International Journal of Management IT & Engineering 216. ”

<sup>42</sup> “A Kolk and J Pinkse 'The Integration of Corporate Governance in Corporate Social Responsibility Disclosures' (2010) 18 Corporate Social Responsibility and Environmental Management 15. ”

<sup>43</sup> “S Benn and D Bolton Key Concepts in Corporate Social Responsibility (Sage Publications 2011). ”

<sup>44</sup> “B Tricker Corporate Governance: Principles Policies and Practices (3rd edn Oxford University Press 2015). ”

<sup>45</sup> “A Kakabadse N Kakabadse and L Lee-Davies 'CSR Leaders Road-Map' (2009) 2 Corporate Governance 9. ”

<sup>46</sup> “R Sharma 'Role of Board of Directors in Corporate Social Responsibility' (2013) 2 International Journal of Management & Business Studies 47. ”

<sup>47</sup> “RE Freeman and others Stakeholder Theory: The State of the Art (Cambridge University Press 2010). ”

<sup>48</sup> “J Andriof and others (eds) Unfolding Stakeholder Thinking 2: Relationships Communication Reporting and Performance (Routledge 2017). ”

<sup>49</sup> “AccountAbility AA1000 Stakeholder Engagement Standard (AccountAbility 2015). ”

stakeholder interests companies can build trust enhance their social license to operate and create shared value”.<sup>50</sup>

### *2. Improved communication and transparency with stakeholders*

CSR promotes improved communication and transparency between companies and their stakeholders. Companies are increasingly publishing sustainability reports disclosing their CSR activities and engaging in regular dialogue with stakeholders.<sup>51</sup> “Transparency allows stakeholders to assess a company's CSR performance hold them accountable and make informed decisions”.<sup>52</sup> Effective communication helps build relationships foster collaboration and align stakeholder expectations with business objectives.<sup>53</sup>

## **D. CSR and risk management**

### *1. Reputational risks*

CSR plays a vital role in managing reputational risks for companies. “In today's interconnected world companies face increased scrutiny from media civil society organizations” and the public at large.<sup>54</sup> Negative publicity related to unethical practices environmental damage or social irresponsibility “can severely damage a company's reputation and brand value”.<sup>55</sup> By proactively addressing CSR issues and demonstrating responsible behavior companies can mitigate reputational risks and protect their brand image.<sup>56</sup>

### *2. Legal and regulatory risks*

CSR helps companies manage “legal and regulatory risks associated with non-compliance or unethical practices. With the introduction of mandatory CSR requirements under the Companies Act 2013 Indian companies face legal obligations to engage in CSR activities and report on their

---

<sup>50</sup> “ME Porter and MR Kramer 'Creating Shared Value' (2011) 89 Harvard Business Review 62. ”

<sup>51</sup> “KPMG 'The KPMG Survey of Sustainability Reporting 2022' accessed 20 April 2023. ”

<sup>52</sup> “Global Reporting Initiative 'GRI Standards' accessed 20 April 2023. ”

<sup>53</sup> “J Kujala A Rehbein and T Toikka 'Communicating Corporate Social Responsibility' in A Rasche M Morsing and J Moon (eds) Corporate Social Responsibility: Strategy Communication Governance (Cambridge University Press 2017)”

<sup>54</sup> “C Fombrun and M Shanley 'What's in a Name? Reputation Building and Corporate Strategy' (1990) 33 Academy of Management Journal 233. ”

<sup>55</sup> “N Esen 'Managing and Measuring Corporate Reputation' (2013) 1 International Business Research 95. ”

<sup>56</sup> “CB Bhattacharya and S Sen 'Doing Better at Doing Good: When Why and How Consumers Respond to Corporate Social Initiatives' (2004) 47 California Management Review 9. ”

initiatives.<sup>57</sup> Non-compliance with CSR provisions can lead to penalties and legal consequences.<sup>58</sup> Moreover companies that engage in unethical or illegal practices face the risk of regulatory action legal liabilities and financial losses.<sup>59</sup> By integrating CSR into their risk management frameworks companies can ensure compliance” with legal requirements and minimize exposure to legal and regulatory risks.<sup>60</sup>

## **CSR IMPLEMENTATION AND CORPORATE GOVERNANCE PRACTICES**

### **A. Integration of CSR into corporate strategy and governance structures**

Integrating CSR into corporate strategy and governance structures is crucial for effective implementation. “Companies are increasingly recognizing the importance of aligning their CSR initiatives with their overall business objectives and values.<sup>61</sup> This integration involves incorporating CSR considerations into decision-making processes risk management frameworks and performance evaluation systems.<sup>62</sup> By embedding CSR into the core of their operations companies can ensure that it becomes an integral part of their corporate culture” and identity.<sup>63</sup>

#### *1. CSR committees and their role*

The formation of CSR committees at the board level is a key mechanism for integrating CSR into governance structures.<sup>64</sup> “CSR committees are responsible for overseeing the development implementation and monitoring of CSR policies and programs.<sup>65</sup> They play a crucial role in setting the strategic direction for CSR allocating resources and ensuring compliance with legal

---

<sup>57</sup> “The Companies Act 2013 s 135 and the Companies (Corporate Social Responsibility Policy) Rules 2014. ”

<sup>58</sup> “Ministry of Corporate Affairs 'General Circular No. 01/2016' (12 January 2016). ”

<sup>59</sup> “S Goel and N Ramanathan 'Business Ethics and Corporate Social Responsibility – Is there a Dividing Line?' (2014) 11 *Procedia Economics and Finance* 49. ”

<sup>60</sup> “R Ullah 'Corporate Governance and Risk Management: A Proposed Framework for CSR Compliance' (2015) 10 *International Journal of Business and Management* 187. ”

<sup>61</sup> “R Panda and NM Modak 'Corporate Social Responsibility: Conceptual Framework and Strategies for Sustainable Development' in NM Modak (ed) *Corporate Social Responsibility in India: Cases and Developments after the Legal Mandate* (Springer 2016). ”

<sup>62</sup> “A Kolk 'Sustainability Accountability and Corporate Governance: Exploring Multinationals' Reporting Practices' (2008) 18 *Business Strategy and the Environment* 1. ”

<sup>63</sup> “S Benn and D Bolton *Key Concepts in Corporate Social Responsibility* (Sage Publications 2011). ”

<sup>64</sup> “RM Hanson 'The Role of the Board of Directors in Corporate Governance' (2014) 29 *Corporate Governance Advisor* 1. ”

<sup>65</sup> “The Companies Act 2013 s 135(1). ”

requirements”.<sup>66</sup> CSR committees also facilitate regular reporting to the board on CSR performance and provide guidance on stakeholder engagement and communication.<sup>67</sup>

## *2. CSR policies and reporting mechanisms*

Developing comprehensive CSR policies and reporting mechanisms is essential for effective CSR implementation. CSR policies “provide a framework for guiding the company's CSR activities and ensuring consistency and alignment with business objectives”.<sup>68</sup> These policies should clearly define the company's CSR priorities goals and implementation strategies.<sup>69</sup> Robust reporting mechanisms such as sustainability reports and integrated reports enable companies to communicate their CSR performance to stakeholders transparently.<sup>70</sup> “Regular reporting helps companies track their progress identify areas for improvement and demonstrate accountability”.<sup>71</sup>

## **B. Board diversity and CSR**

### *1. Importance of diverse perspectives in CSR decision-making*

Board “diversity plays a significant role in enhancing CSR decision-making and oversight. A diverse board brings a range of perspectives experiences and expertise to the table which can lead to more comprehensive and inclusive CSR strategies.<sup>72</sup> Diversity in terms of gender age ethnicity and professional background helps ensure that various stakeholder interests are considered and addressed”.<sup>73</sup> Diverse boards are more likely to challenge traditional thinking foster innovation and promote a broader understanding of social and environmental issues.<sup>74</sup>

### *2. Women directors and their impact on CSR initiatives*

“The presence of women directors on corporate boards has been linked to improved CSR performance. Studies have shown that companies with a higher proportion of women directors tend

---

<sup>66</sup> “R Sharma 'Role of Board of Directors in Corporate Social Responsibility' (2013) 2 International Journal of Management & Business Studies 47. ”

<sup>67</sup> “B Tricker Corporate Governance: Principles Policies and Practices (3rd edn Oxford University Press 2015).”

<sup>68</sup> “Sunil Misser CSR Reporting & Analysis (2020) ”

<sup>69</sup> “FICCI Aditya Birla CSR Centre for Excellence The Handbook on Corporate Social Responsibility in India (2016) ”

<sup>70</sup> “KPMG 'The KPMG Survey of Sustainability Reporting in India 2020”

<sup>71</sup> “Global Reporting Initiative 'GRI Standards' accessed 20 April 2023. ”

<sup>72</sup> “S Bear N Rahman and C Post 'The Impact of Board Diversity and Gender Composition on Corporate Social Responsibility and Firm Reputation' (2010) 97 Journal of Business Ethics 207. ”

<sup>73</sup> “TF Cooke 'Top Management Team Diversity: Implications for Corporate Social Responsibility' in LJ de Jongh and others (eds) The Palgrave Handbook of Corporate Social Responsibility (Palgrave Macmillan 2022) ”

<sup>74</sup> “R Isidro 'The Relationship Between Women Directors and Corporate Social Responsibility' (2013) 23 Journal of Business Ethics 144. ”

to have stronger CSR initiatives and better stakeholder engagement”.<sup>75</sup> Women directors often bring a different perspective and are more likely to prioritize issues related to social responsibility sustainability and ethical conduct.<sup>76</sup> They also tend to be more empathetic and focused on building relationships with stakeholders.<sup>77</sup> The inclusion of women on boards can lead to more effective CSR decision-making and implementation.<sup>78</sup>

### **C. Executive compensation and CSR performance**

#### *1. Linking CSR metrics to executive pay*

Linking CSR metrics to executive compensation is an emerging trend in corporate governance. By tying a portion of executive pay to “CSR performance companies can incentivize and reward executives for their contributions to social and environmental goals.”<sup>79</sup> This approach aligns the interests of executives with those of stakeholders and encourages a long-term perspective on value creation.<sup>80</sup> CSR metrics can include targets related to carbon emissions reduction diversity and inclusion employee engagement and community impact.<sup>81</sup> Incorporating CSR metrics into executive compensation plans demonstrates a company's commitment to responsible business practices”.<sup>82</sup>

#### *2. Balancing financial and non-financial incentives*

Balancing financial and “non-financial incentives is crucial for promoting a holistic approach to CSR and corporate governance”. While financial incentives such as bonuses and stock options remain important for motivating executives non-financial incentives are equally valuable.<sup>83</sup> Non-financial

---

<sup>75</sup> “DG Kang and A Sorensen 'The Impact of Board Gender Diversity on Corporate Social Responsibility' (2017) 9 Academy of Management Annual Meeting Proceedings. ”

<sup>76</sup> “R Arora 'Women Directors and Corporate Social Responsibility: An Analytical Study in the Indian Context' (2022) 7 SJCC Management Research Review 56. ”

<sup>77</sup> “L Azmi AR Khan and S Alam 'Impact of Gender Diversity in Board on Firm Performance and Corporate Social Responsibility' (2021) 17 Vidyasagar University Journal of Commerce 66. ”

<sup>78</sup> “T Lambooy and others 'The Role of Women in Corporate Governance and Sustainability: An International Perspective' in M Aluchna and SY Idowu (eds) The Dynamics of Corporate Social Responsibility (Springer 2017). ”

<sup>79</sup> “FEG Otten and R Weber 'Integrating Sustainability into Managerial Incentive Schemes: A Case Study Analysis' (2019) 13 Journal of Management and Sustainability 116. ”

<sup>80</sup> “S Mahapatra 'Aligning Corporate Social Responsibility with Executive Compensation' (2019) 6 International Journal of Management Studies 4. ”

<sup>81</sup> “V Maas 'The Effect of Corporate Social Performance on Corporate Financial Performance: A Review and Research Agenda' (2015) 132 Journal of Business Ethics 293. ”

<sup>82</sup> “M Bruhl 'Linking Executive Compensation to Sustainability Performance: A Path to Aligning Interests' in S Boubaker D Cumming and DK Nguyen (eds) Research Handbook of Finance and Sustainability (Edward Elgar Publishing 2018). ”

<sup>83</sup> “DR Kaplan 'Pay for Environmental Social and Governance (ESG) Performance' (2020) 32 Journal of Applied Corporate Finance 64. ”

incentives can include recognition career advancement opportunities and the intrinsic satisfaction of contributing to social and environmental causes.<sup>84</sup> Striking the right balance between financial and non-financial incentives helps ensure that “executives are not solely focused on short-term financial gains but also consider the long-term sustainability and social impact of their decisions”.<sup>85</sup>

## **CHALLENGES AND CRITICISMS**

### **A. Balancing CSR and financial performance**

“One of the main challenges faced by companies in implementing CSR is balancing social and environmental responsibilities with financial performance. There is often a perception that investing in CSR initiatives comes at the cost of profitability and shareholder value.<sup>86</sup> However research has shown that companies with strong CSR practices can enhance their financial performance in the long run through improved reputation risk management and stakeholder loyalty”.<sup>87</sup> Finding the right balance between CSR and financial goals requires strategic planning effective resource allocation and a long-term perspective on value creation.<sup>88</sup>

### **B. Greenwashing and CSR as a PR exercise**

“Greenwashing which refers to the practice of making misleading or false claims about a company's environmental or social performance is a significant criticism of CSR”.<sup>89</sup> Some companies may engage in CSR activities primarily as a public relations exercise to enhance their image and reputation without genuine commitment to responsible business practices.<sup>90</sup> Greenwashing can erode stakeholder trust damage corporate reputation and undermine the credibility of CSR efforts.<sup>91</sup> To

---

<sup>84</sup> “M Painter-Morland 'Triple Bottom-Line Reporting as Social Grammar: Integrating Corporate Social Responsibility and Corporate Codes of Conduct' (2006) 15 Business Ethics: A European Review 352. ”

<sup>85</sup> “S Brammer and A Millington 'Corporate Reputation and Philanthropy: An Empirical Analysis' (2005) 61 Journal of Business Ethics 29. ”

<sup>86</sup> “M Friedman 'The Social Responsibility of Business is to Increase its Profits' The New York Times Magazine (13 September 1970). ”

<sup>87</sup> “CB Bhattacharya and S Sen 'Doing Better at Doing Good: When Why and How Consumers Respond to Corporate Social Initiatives' (2004) 47 California Management Review 9. ”

<sup>88</sup> “A Karnani Doing Well by Doing Good: The Grand Illusion (2011) 53 California Management Review 69.

<sup>89</sup> “W Visser The Age of Responsibility: CSR 2.0 and the New DNA of Business (John Wiley & Sons 2011). ”

<sup>90</sup> “F Bowen After Greenwashing: Symbolic Corporate Environmentalism and Society (Cambridge University Press 2014). ”

<sup>91</sup> “S Mahoney and others 'A Review of Research on the Negative Accounting Relationship between Risk and Return: Bowman's Paradox' (2013) 30 Omega 1. ”

address this issue companies need to ensure transparency accountability and third-party verification of their CSR claims and initiatives.<sup>92</sup>

### **C. Lack of standardization in CSR reporting and metrics**

The lack of standardization in CSR reporting and metrics poses challenges for comparability and accountability. “Different companies may use varying frameworks indicators and methodologies for measuring and reporting their CSR performance making it difficult for stakeholders to assess and compare the impact of CSR initiatives across organizations”.<sup>93</sup> The absence of globally accepted standards for CSR reporting can lead to inconsistencies cherry-picking of favorable metrics and a lack of transparency.<sup>94</sup> “Efforts are being made by international organizations and standard-setting bodies to develop harmonized CSR reporting frameworks such as the Global Reporting Initiative (GRI) and the Sustainability Accounting Standards Board (SASB)”.<sup>95</sup>

### **D. Enforcement and accountability concerns**

Enforcement and accountability concerns are prevalent in the CSR landscape. While the Companies Act 2013 mandates CSR spending and reporting for certain companies the enforcement mechanisms and penalties for non-compliance are often perceived as weak or inadequate.<sup>96</sup> The lack of strict enforcement can lead to non-compliance misreporting or superficial CSR activities.<sup>97</sup> Moreover holding companies accountable for their CSR commitments and the impact of their initiatives remains a challenge.<sup>98</sup> Strengthening enforcement measures imposing stricter penalties and enhancing stakeholder scrutiny can help improve accountability and ensure genuine commitment to CSR.<sup>99</sup>

---

<sup>92</sup> “S Prakash Sethi and others 'Faking It: Brand Integrity and the Question of Greenwashing' in S Prakash Sethi (ed) Globalization and Self-Regulation: The Crucial Role That Corporate Codes of Conduct Play in Global Business (Palgrave Macmillan 2011). ”

<sup>93</sup> “RG Eccles and others 'The Impact of Corporate Sustainability on Organizational Processes and Performance' (2014) 60 Management Science 2835. ”

<sup>94</sup> “J Dando and T Swift 'Transparency and Assurance: Minding the Credibility Gap' (2003) 44 Journal of Business Ethics 195. ”

<sup>95</sup> “A Kolk 'Sustainability Reporting: Insights from International Standardization' in J Bebbington B O'Dwyer and J Unerman (eds) Sustainability Accounting and Accountability (2nd edn Routledge 2014). ”

<sup>96</sup> “PK Halder and S Mishra 'The Changing Facets of Corporate Governance and Corporate Social Responsibility in India and Their Interrelationship' (2015) 14 Journal of Corporate Governance 95. ”

<sup>97</sup> “CSR Box 'Key Challenges in CSR Reporting' accessed 20 April 2023. ”

<sup>98</sup> “GK Kapoor and S Dharmija 'Mandatory CSR Spending—Indian Experience' (2017) 4 Emerging Economy Studies 98. ”

<sup>99</sup> “J Moon 'The Social Responsibility of Business and New Governance' (2007) 3 Government and Opposition 370. ”

## **CASE STUDIES**

### **A. Tata Group: A pioneer in CSR and corporate governance in India**

“The Tata Group one of India's largest and most respected conglomerates has been a pioneer in CSR and corporate governance practices. The group's founder Jamsetji Tata believed in the concept of trusteeship and the responsibility of businesses towards society.<sup>100</sup> The Tata Group has a long history of philanthropic activities community development initiatives and ethical business practices”.<sup>101</sup> The group has established various trusts and foundations such as the Tata Trusts and the Tata Institute of Social Sciences to promote social welfare and development.<sup>102</sup> The Tata Group's corporate governance framework emphasizes transparency accountability and stakeholder engagement setting a benchmark for other Indian companies.<sup>103</sup>

### **B. Infosys: Integrating CSR into core business operations**

Infosys a leading “Indian information technology company has successfully integrated CSR into its core business operations. The company's CSR initiatives are aligned with its business expertise and focus on areas such as education digital literacy and environmental sustainability”.<sup>104</sup> Infosys has established the Infosys Foundation which works towards eradicating hunger promoting education and improving healthcare in rural communities.<sup>105</sup> “The company also has a robust corporate governance framework with a strong emphasis on ethics transparency and risk management.<sup>106</sup> Infosys' integrated approach to CSR and corporate governance has earned it recognition as one of the most respected and socially responsible companies in India”.<sup>107</sup>

### **C. ITC Limited: Sustainable agriculture and rural development initiatives**

ITC Limited a diversified conglomerate with interests in consumer goods agriculture and hospitality has made significant contributions to sustainable agriculture and rural development through its CSR initiatives. The company's "e-Choupal" program has revolutionized the way farmers access

---

<sup>100</sup> “S Ramesh and K Mendes 'Corporate Social Responsibility of Tata Group' (2015) 3 International Journal of Engineering and Management Research 111. ”

<sup>101</sup> “Tata Group 'Community & Sustainability' accessed 20 April 2023. ”

<sup>102</sup> “KN Nair and A Sodhi 'TISS: A Role Model for Corporate Social Responsibility' (2011) 40 Vikalpa 97. ”

<sup>103</sup> “Tata Group 'Corporate Governance' accessed 20 April 2023. ”

<sup>104</sup> “Infosys 'Corporate Social Responsibility' accessed 20 April 2023. ”

<sup>105</sup> “Infosys 'Infosys Foundation' accessed 20 April 2023. ”

<sup>106</sup> “Infosys 'Corporate Governance Report 2022' accessed 20 April 2023. ”

<sup>107</sup> “Forbes India 'Infosys' CSR Initiatives Focus on Enriching People's Lives' (14 March 2022). ”

information products and services empowering them and improving their livelihoods.<sup>108</sup> ITC's "Watershed Development" program focuses on soil and water conservation afforestation and sustainable agricultural practices in rural areas.<sup>109</sup> The company also promotes women's empowerment and provides vocational training to youth in rural communities.<sup>110</sup> "ITC's CSR initiatives are closely aligned with its business strategy of creating value for all stakeholders including farmers communities and the environment".<sup>111</sup>

## **RECOMMENDATIONS FOR STRENGTHENING CSR AND CORPORATE GOVERNANCE**

### **A. Enhancing board oversight and accountability for CSR**

To strengthen "CSR and corporate governance it is essential to enhance board oversight and accountability for CSR". Boards should take an active role in setting the CSR agenda monitoring CSR performance and ensuring that CSR is integrated into the overall business strategy.<sup>112</sup> Boards should establish dedicated CSR committees with clear responsibilities and regular reporting mechanisms.<sup>113</sup> Board members should have the necessary expertise and training to effectively oversee CSR initiatives and assess their impact.<sup>114</sup> Holding boards accountable for CSR performance through performance evaluations and stakeholder feedback can further enhance their commitment to responsible business practices.<sup>115</sup>

### **B. Improving CSR disclosure and reporting standards**

Improving CSR disclosure and reporting standards is crucial for enhancing transparency comparability and accountability. "Companies should adopt internationally recognized reporting frameworks such as the GRI Standards or the Integrated Reporting Framework to ensure consistency and credibility in their CSR reporting".<sup>116</sup> Mandatory CSR reporting requirements should be

---

<sup>108</sup> "ITC Limited 'Sustainability Initiatives' accessed 20 April 2023. "

<sup>109</sup> "ITC Limited 'Watershed Development' accessed 20 April 2023. "

<sup>110</sup> "ITC Limited 'Women's Empowerment' accessed 20 April 2023. "

<sup>111</sup> "ITC Limited 'Business Responsibility Report 2022' accessed 20 April 2023. "

<sup>112</sup> "B Tricker Corporate Governance: Principles Policies and Practices (3rd edn Oxford University Press 2015). "

<sup>113</sup> "The Institute of Company Secretaries of India 'Corporate Social Responsibility' accessed 20 April 2023. "

<sup>114</sup> "JA Walls and others 'Corporate Governance and Environmental Performance: Is there really a link?' (2012) 33 Strategic Management Journal 885. "

<sup>115</sup> "RM Hanson 'The Role of the Board of Directors in Corporate Governance' (2014) 29 Corporate Governance Advisor 1. "

<sup>116</sup> "AccountAbility AA1000 Stakeholder Engagement Standard (AccountAbility 2015). "

strengthened with clear guidelines on the content format and verification of CSR reports.<sup>117</sup> Third-party assurance of CSR reports can enhance their reliability and build stakeholder trust.<sup>118</sup> Encouraging the adoption of standardized CSR metrics and key performance indicators (KPIs) can facilitate “benchmarking and enable stakeholders to make informed assessments of CSR performance”.<sup>119</sup>

### **C. Encouraging stakeholder engagement and dialogue**

Effective stakeholder engagement and dialogue are essential for understanding stakeholder expectations addressing their concerns and fostering collaborative relationships. “Companies should establish formal mechanisms for stakeholder engagement such as stakeholder advisory panels regular stakeholder meetings and grievance redressal systems.<sup>120</sup> Engaging with a diverse range of stakeholders including employees customers suppliers local communities and civil society” organizations can provide valuable insights and inform CSR strategies.<sup>121</sup> Transparent communication and regular feedback loops can help build trust and ensure that CSR initiatives are responsive to stakeholder needs.<sup>122</sup> Collaborating with stakeholders on CSR projects and initiatives can lead to more impactful and sustainable outcomes.<sup>123</sup>

### **D. “Promoting a culture of ethical leadership and responsible business practices”**

Promoting a culture of ethical leadership and responsible business practices is fundamental for embedding CSR into the core of corporate governance. “Top management and the board should set the tone at the top by demonstrating a strong commitment to ethics integrity and social responsibility.<sup>124</sup> Ethical values and CSR principles should be integrated into the company's mission vision and code of conduct”.<sup>125</sup> Regular training and awareness programs on business ethics and CSR

---

<sup>117</sup> “Ministry of Corporate Affairs 'National Voluntary Guidelines on Social Environmental and Economic Responsibilities of Business' (2011). ”

<sup>118</sup> “KPMG 'The KPMG Survey of Sustainability Reporting in India 2020'. ”

<sup>119</sup> “Global Reporting Initiative and the United Nations Global Compact 'Business Reporting on the SDGs: An Analysis of the Goals and Targets' (2017). ”

<sup>120</sup> “AA1000 Stakeholder Engagement Standard (2015). ”

<sup>121</sup> “R Edward Freeman Strategic Management: A Stakeholder Approach (Pitman 1984). ”

<sup>122</sup> “J Andriof and S Waddock 'Unfolding Stakeholder Engagement' in J Andriof and others (eds) Unfolding Stakeholder Thinking: Theory Responsibility and Engagement (Routledge 2002). ”

<sup>123</sup> “B Rasche and D Esser 'From Stakeholder Management to Stakeholder Accountability' (2006) 65 Journal of Business Ethics 251. ”

<sup>124</sup> “LK Trevino and others 'Managing Ethics and Legal Compliance: What Works and What Hurts' (1999) 41 California Management Review 131. ”

<sup>125</sup> “WM Greenfield 'Ethics and Corporate Social Responsibility in Business' in WM Greenfield (ed) Morality and the Market (Routledge 2019). ”

should be conducted for employees at all levels.<sup>126</sup> Recognizing and rewarding employees who exemplify ethical behavior and contribute to CSR initiatives can reinforce a culture of responsibility.<sup>127</sup> Encouraging open communication whistleblowing mechanisms and a speak-up culture can help identify and address unethical practices.<sup>128</sup>

## **CONCLUSION & SUGGESTIONS**

### **A. Recap of the key findings on the “impact of CSR on corporate governance”**

This research paper has explored the “impact of Corporate Social Responsibility (CSR)” on corporate governance practices in India. The key findings suggest that CSR has a significant influence on various aspects of corporate governance including board decision-making stakeholder engagement risk management and corporate strategy. The integration of CSR into governance structures through mechanisms such as CSR committees and policies has become increasingly prevalent in Indian companies. Board diversity particularly the presence of women directors has been associated with improved CSR performance and stakeholder orientation. Linking CSR metrics to executive compensation is an emerging trend that aligns managerial incentives with social and environmental objectives.

### **B. Outlook for “CSR and corporate governance in India”**

“Outlook for CSR and corporate governance in India is promising with a growing recognition of the importance of responsible business practices”. The Companies Act 2013 has been a significant step towards mandating CSR and enhancing corporate accountability. However challenges such as balancing CSR and financial performance preventing greenwashing and ensuring effective enforcement and accountability mechanisms persist. As stakeholder expectations evolve and global sustainability challenges intensify Indian companies will need to adapt and strengthen their CSR and governance practices. Collaboration between businesses government and civil society will be crucial in driving systemic change and creating a more sustainable and inclusive economy.

---

<sup>126</sup> “LK Trevino and KA Nelson *Managing Business Ethics: Straight Talk about How to Do It Right* (7th edn John Wiley & Sons 2017).”

<sup>127</sup> “ML Markham 'The Role of Corporate Ethics and Compliance Programs in The Governance of Corporations' in GJ Rossouw and A van Vuuren (eds) *Business Ethics* (5th edn Oxford University Press 2013).”

<sup>128</sup> “R Batory and others 'Whistleblowing and Ethics Helplines' in R Maehle (ed) *Ethics and Compliance Programs in Multinational Organizations* (Springer Gabler 2012).”

### **C. Importance of aligning CSR and corporate governance for “long-term sustainability and value creation”**

Aligning “CSR and corporate governance is essential for achieving long-term sustainability and value creation”. By integrating “CSR into the core of business operations and decision-making processes companies can better manage risks seize opportunities and create shared value for all stakeholders. A robust corporate governance framework that prioritizes transparency accountability and ethical behavior provides the foundation for effective CSR implementation”. When CSR and corporate governance are aligned companies are better positioned to address social and environmental challenges build trust with “stakeholders and contribute to sustainable development. Ultimately the integration of CSR and corporate governance is not only a moral imperative but also a strategic necessity for businesses to thrive in an increasingly complex and interconnected world”.

## **"FAKING REALITY, REAL CONSEQUENCES: REGULATING DEEPAKES AND SEXTORTION IN THE DIGITAL AGE"**

Divya Girsra\*  
Preeti Deswal\*\*

---

### **ABSTRACT**

Deepfake technology has become both a wonder of ingenuity and a tool for digital abuse in a time when synthetic media and algorithmic manipulation are becoming more and more prevalent. This article examines the startling increase in deepfakes and how they relate to sextortion, a forceful sexual exploitation tactic that uses convincingly faked material rather than actual intimate stuff. Deepfakes, which are made possible by artificial intelligence and machine learning, allow offenders to produce incredibly lifelike but completely fraudulent sexual photos or films, frequently without the target's knowledge or agreement. Even though the events shown never happened, the psychological and reputational harm is severe when such content is used to threaten, blackmail, or degrade victims.

This study explores the technical processes that produce deepfakes, the increasing frequency of sextortion motivated by deepfakes, and the particular moral and legal issues they raise. It critically analyses India's disjointed legal system, which includes the Information Technology Act and the Indian Penal Code. These laws provide some protection, but they are unable to address the precise kind and speed of harm caused by AI. The article illustrates the global lack of laws specifically designed to address non-consensual synthetic sexual material through comparative analysis from countries such as the US, UK, and EU.

The article suggests a thorough regulatory plan for India to address these deficiencies. The adoption of a specific law addressing deepfakes and digital sexual assault, changes to current IT regulations to cover AI-generated content, funding for deepfake detection systems, and international collaboration through frameworks like the Budapest Convention are some of the main

---

\* Research Scholar, Guru Gobind Singh Indraprastha University (IP University)

\*\* Assistant Professor, Innovation Institute of law

recommendations. In order to counter this new threat, the study also highlights the significance of victim-centered solutions, platform responsibility, public awareness, and digital literacy.

## **1. INTRODUCTION**

Truth is no longer a fixed reality in the digital age; it can be easily created, copied, and altered. Deepfake technology, a new artificial intelligence-powered tool that makes it possible to create incredibly lifelike but completely fake audio, video, and image content, is at the centre of this change. What started out as a gaming and entertainment innovation has quickly evolved into a weapon of abuse, deceit, and false information.

Deepfakes create information that can make someone appear to say or do things they never did by using machine learning techniques, especially Generative Adversarial Networks (GANs). Many deepfakes are weaponized, although some are used for innocent experimentation or parody. By using their faces in sexually explicit videos or creating naked photographs from photos of people wearing clothing without their knowledge, they are increasingly being exploited to attack people, particularly women. The victim is then threatened, blackmailed, or shamed as a result of this exploitation, which frequently takes place in intimate settings. As a result, the deepfake turns into a tool for online sexual aggression, where the fake seems just as offensive as the real thing. Sextortion, another rising cybercrime, has a troubling junction with this manipulation of synthetic media. In order to extort, harass, or intimidate their victims, offenders increasingly create deepfakes of sexual content instead of relying on real sexual content. The delusion alone is sufficient in this type of abuse to ruin reputations, cause pain, and keep victims in vicious cycles of silence and dread. The harm is still achingly palpable, even though the boundaries between reality and fiction are blurred.

## **2. WHAT IS SEXTORTION?**

A type of coercive sexual abuse known as sextortion occurs when abusers threaten to reveal a victim's private or sexual material, whether it be synthetic or real, unless demands are fulfilled. These requests could include money payments, the sharing of explicit material going forward, or following sexual orders or favors. Sextortion has entered a new phase, where victims may not have produced any sexual content at all, but still face terrible repercussions, thanks to the development of AI technologies that can construct sexually explicit content from a public selfie.

Sextortion is frequently carried out anonymously, internationally, and at a startling rate, in contrast to more conventional sexual transgressions. Despite never having seen the victim, the criminal can

intimidate them via a screen by threatening to send manipulated videos to friends, relatives, or employers. The psychological toll is exacerbated by the dread of disbelief—"What if no one believes it's fake?"—especially when there is a significant level of social or cultural shame associated with sexuality.

Victims of deepfake-driven sextortion risk not just emotional and reputational harm, but often legal difficulties as well. The production or dissemination of deepfakes is not expressly illegal in many areas, especially when the content is synthetic yet seems sexual. When this happens, victims are left unprotected and justice is either postponed or denied because the law is unable to keep up with technological advancements.

This article explores this developing concern, concentrating on the moral, legal, and regulatory issues raised by deepfake technology when it is employed as a means of sexual harassment and sextortion. It compares international approaches, examines how contemporary legal systems—especially in India—handle (or fail to address) this issue, and makes policy recommendations to fortify the regulatory environment. It is more important than ever to preserve human autonomy, consent, and dignity as we negotiate this artificial world.

### **3. UNDERSTANDING DEEPPAKES AND SEXTORTION**

Deepfake technology, a type of synthetic media produced with artificial intelligence (AI), especially deep learning models like Generative Adversarial Networks (GANs), has rapidly proliferated in the digital world in recent years. The goal of deepfakes is to create an uncanny sense of realism by superimposing pre-existing images, audio, or video content onto source materials. Two AI models are at the centre of this process: the generator, which creates increasingly realistic false media, and the discriminator, which assesses its authenticity. The machine can create content that is almost identical to real footage thanks to this adversarial training. Although the technology has valid applications in accessibility, education, and filmmaking, it has swiftly turned into a weapon for abuse, deceit, and manipulation.

Viral parody videos and novelty apps like FaceApp, which digitally imitated celebrities like Tom Cruise and Barack Obama, were the first to introduce deepfakes into popular culture. But now that open-source deepfake tools are widely available, this technology has become more accessible,

enabling even those with no technical knowledge to produce lifelike fake videos. The potential for abuse is enormous. The production of non-consensual pornographic deepfakes, in which people—typically women—are digitally added to sexually explicit videos or have their faces superimposed on nude bodies, is a particularly alarming development. A 2019 study by Sensity AI<sup>1</sup> found that more than 90% of the targets of deepfake movies on the internet are women, including journalists, celebrities, and increasingly private citizens. Additionally, over 96% of these videos are pornographic in nature.

When used as a tool for sextortion—a type of cyber-enabled sexual blackmail in which people are forced into compliance under threat of exposure—deepfakes become even more hazardous. According to Interpol and cybercrime experts, sextortion is when victims are threatened with the release of intimate photographs<sup>2</sup> or films until they comply with a demand, which is typically money, more explicit content, or even offline sexual favors. Sextortion has historically involved actual content that was either stolen or forced. However, the advent of deepfake technology has made it possible for criminals to participate in blackmail without the necessity for real intimate material. To threaten the victim, they simply require a public image, usually taken from social media, that has been digitally altered to look like a realistic nude photo or video of a sexual act.

The distinction between fabrication and reality is blurred by this artificial sextortion. Victims frequently lack the ability to demonstrate that the material is false, particularly when the visuals are very convincing. In one notorious instance, a teenage girl's Facebook photo was stolen and converted into a naked deepfake by a Telegram bot in India. Even though she had never downloaded or shared any sexual content herself, the phony image spread among her peers, causing psychological distress and suicide thoughts. Such occurrences have sharply increased, according to the National Commission for Women (NCW) and cyber police, especially during the COVID-19 epidemic when increased screen time and digital reliance led to a surge in online harassment.

This is not just an Indian problem. Deepfake sextortion has been used against high school and college students in the United States, frequently by anonymous attackers on websites like Snapchat, Reddit, or Discord. One well-known instance is the deepfake controversy in Bucks County, Pennsylvania (2021), in which a teenage girl utilized deepfake technology<sup>3</sup> to produce compromising

---

<sup>1</sup> *The State of Deepfakes: 2019 Report*, (2019), available at <https://sensity.ai/reports> (last visited Jul. 31, 2025).

<sup>2</sup> **Interpol**, *Understanding Sextortion: Emerging Trends*, (2022), available at <https://www.interpol.int> (last visited Jul. 31, 2025).

<sup>3</sup> **Bucks County District Attorney's Office**, *Press Release on Deepfake Cheerleader Case*, (Mar. 2021), available at <https://www.buckscounty.gov> (last visited Jul. 31, 2025).

and explicit films of her cheerleading competitors in an attempt to disqualify them. This instance demonstrated how deepfakes can be used as a weapon for harassment, manipulation, and personal retaliation, even though there was no money extortion involved.

The impact of deepfake-driven sextortion on reputation, legality, and psychology is what makes it so concerning. Anxiety, sadness, self-harm, and extreme social disengagement are all possible outcomes for victims. Even creating a false image might result in ostracism, marital dissolution, or even honour-based violence in societies where a woman's perceived modesty or sexual behaviour is strongly linked to her family's honour. Furthermore, once the content is online, it is almost impossible to stop the harm due to its viral nature and the lack of effective legal tools for prompt removal or prosecution.

Deepfakes' "believability crisis" further complicates matters. It is frequently the victim's responsibility to demonstrate that the content is fraudulent, even if it is. This presents difficult issues with regard to intent, permission, and evidence from a legal standpoint. For example, prosecutors may find it difficult to use antiquated defamation or obscenity statutes that were never intended for AI-generated lies if there are no explicit laws that expressly forbid deepfakes. This issue has gotten significantly worse due to the proliferation of programs like "Deep Nude" (now prohibited but still in use in cloned versions) and Telegram bots that use artificial intelligence to create nudities in less than 30 seconds. These technologies frequently operate on anonymous platforms or the dark web, which makes it very challenging to find the offender and bring about punishment. They also expose an unsettling business strategy: certain apps use a "pay-to-generate" approach, which commodifies abuse by providing deepfake porn services that require a subscription.

In this dynamic digital environment, consent, dignity, and individual autonomy are frequently violated without physical contact, and truth has become negotiable. When oppressive power structures and technical capabilities collide in the form of deepfake-based sextortion, women and marginalized groups are disproportionately harmed. In order to ensure accountability, justice, and digital safety, the ensuing sections will examine how national and international legal institutions are addressing this unprecedented challenge and identify any remaining inadequacies.

#### **4. LEGAL AND ETHICAL CHALLENGES IN ADDRESSING DEEPFAKES AND SEXTORTION**

One of the most difficult and urgent legal issues in the digital era is the use of deepfake technology in sextortion. A technology that conflates fact and fiction is pushing the boundaries of traditional legal frameworks, which are based on concrete evidence and distinct concepts of privacy and injury. The legal system in many countries, including India, is still insufficient to handle this complex type of gendered cyberviolence, leaving victims vulnerable to serious injury and frequently without a way to get help.

#### **4.1 Gaps in Existing Legal Frameworks**

One of the most immediate challenges in addressing deepfake-based sextortion is the absence of direct legislation specifically criminalizing the creation or distribution of deepfakes for malicious purposes. In India, the Information Technology Act, 2000 (IT Act)<sup>4</sup> and the Bharatiya Nyaya Sanhita, 2023 (BNS) contain provisions that may apply in certain cases but were drafted long before the emergence of synthetic media.

For instance:

Section 66E of the IT Act penalizes the violation of privacy through the capture and transmission of images of private areas without consent.

Section 67 and 67A of the IT Act deal with the publication or transmission of obscene and sexually explicit material in electronic form.

However, these sections implicitly presume that the material in question is real. When the images or videos are artificially generated—as in the case of deepfakes—it becomes legally ambiguous whether these provisions apply.

Under the BNS, 2023, certain sections may offer limited recourse<sup>5</sup>:

Section 63 – criminalizes obscene acts and materials (equivalent to IPC Section 292),

Section 74 – addresses voyeurism (replaces IPC Section 354C),

---

<sup>4</sup> **Information Technology Act, 2000**, Section 66E, 67, 67A.

<sup>5</sup> **Bharatiya Nyaya Sanhita, 2023**, Section 63, 74, 76, 77, 356.

Section 76 – penalizes stalking, including cyberstalking (replaces IPC Section 354D),

Section 77 – deals with insulting the modesty of a woman (replaces IPC Section 509),

Section 356 – covers defamation (replaces IPC Section 499).

However, these again fall short in effectively addressing fabricated synthetic content, especially when the material appears authentic but is entirely artificial. Victims often face significant challenges in establishing harm or proving malicious intent due to the lack of specific legal provisions for deepfakes.

Although the Indian Supreme Court recognized the right to privacy as a fundamental right in Justice K.S. Puttaswamy v. Union of India (2017)<sup>6</sup> under Article 21 of the Constitution, the absence of comprehensive legislative reform tailored to synthetic media means this recognition remains largely symbolic in addressing deepfake-related privacy violations.

#### **4.2 Consent, Autonomy, and Gendered Harm**

The fundamental principles of sexual consent and bodily autonomy are called into question by deepfake sextortion. Long stressed by feminist legal theory, autonomy encompasses the ability to manage one's representation and image. Therefore, even in cases where no physical act has taken place, the non-consensual production and distribution of sexual deepfakes is a type of image-based sexual violence.

In patriarchal cultures like India, where a woman's perceived sexual purity is socially and culturally policed, the harm is exacerbated. Regardless of its veracity, a single fake film or image might result in honour-based violence, family reaction, societal exclusion, forced institutionalization, or even suicide. The Supreme Court correctly invalidated Section 66A of the IT Act in *Shreya Singhal v. Union of India* (2015)<sup>7</sup> for being ambiguous and overbroad, but the ruling also brought attention to the dearth of specific legislative protections against gendered, reputation-damaging, and frequently anonymous online abuse. From an ethical perspective, the problem involves authority and violation in addition to deception. A

---

<sup>6</sup> **Supreme Court of India**, *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.

<sup>7</sup> **Shreya Singhal v. Union of India**, (2015) 5 SCC 1.

fake image that is used to intimidate, suppress, or degrade a woman serves as a tool of digital patriarchy, reaffirming authority over women's bodies even in online environments.

### **4.3 Proof, Forensics, and the Burden of Evidence**

The burden of proof imposed on victims is another essential issue. When it comes to high-quality deepfakes, the judicial system usually needs the complainant to prove that the content is false, which is nearly difficult. Even forensic investigators find it difficult to verify or disprove deepfake content without sophisticated tools due to the quick development of generative AI.

Victims frequently experience victim-blaming, incredulity, or delays in justice. When law enforcement lacks the resources or technical know-how to look into such cases, the situation gets worse. The Delhi High Court recognized the challenge of striking a balance between digital free expression and individual privacy in *Faizan Siddiqui v. State* (2021)<sup>8</sup>, but it also pointed out the lack of precise rules or investigative procedures for new tech-related harms like deep fakes.

Furthermore, the psychological and reputational damage is already done, even if the victim is successful in demonstrating that the content is fraudulent. The memory of the internet is vast; even fake stuff is stored, copied, and occasionally made profitable once it is spread. Traditional legal theories of obscenity and defamation, which presume a retrievable, finite distribution of injury, are upended by this fact.

### **4.4 Free Speech v/s Protection from Harm**

The balance between defending people from abuse and preserving their right to free speech is one of the most challenging ethical and legal issues surrounding deepfakes. The First Amendment sets a high bar for censoring speech, including satire and digital parody, in countries like the US. Laws that attempt to limit deepfakes must therefore be cautious not to go too far in order to prevent the censorship of acceptable political, journalistic, or artistic content. But as academics like Mary Anne Franks and Danielle Citron have pointed out<sup>9</sup>, freedom of expression cannot be sacrificed for the sake of silence. The legal system must acknowledge that

---

<sup>8</sup> **Faizan Siddiqui v. State**, 2021 SCC OnLine Del 4589.

<sup>9</sup> **Danielle Citron and Mary Anne Franks**, *Cyber Civil Rights: Addressing Gender-Based Harms*, 102 CALIF. L. REV. 40 (2019).

deepfakes are speech that causes harm rather than speech that should be protected when they are used to silence, threaten, or blackmail victims—especially women.

Article 19(1)(a) of the Constitution guarantees freedom of expression, even though India does not have an explicit constitutional right to free speech like the United States. However, there are legitimate limitations on this right, such as those pertaining to morality, decency, and public order. Courts must strike this fine balance in the context of deepfake sextortion while keeping gender and rights in mind.

#### **4.5 Jurisdictional and Cross-Border Challenges**

The worldwide, anonymous, and viral nature of deepfake production and dissemination presents perhaps the most difficult obstacle. The criminal is frequently based abroad and uses dark web sites, VPNs, or encrypted platforms (like Telegram or Discord) to disseminate content and avoid detection. Meanwhile, victims of cross-border cyberbullying are frequently left defenceless.

International collaboration options are provided by existing frameworks like the Budapest Convention on Cybercrime (2001)<sup>10</sup>, but India is not a party, and the convention itself does not take synthetic media crimes into account. In circumstances where time is of the essence, such as when a deepfake spreads quickly, the Mutual Legal Assistance Treaty (MLAT) procedure for obtaining foreign evidence is cumbersome, slow, and unsuitable. Furthermore, a lot of IT platforms may not respond to takedown requests because they are based in nations with antiquated or lax regulations on digital material. Platforms may use safe harbour clauses to evade accountability, and enforcement varies even in cases where national laws require intermediary due diligence (such as India's 2021 IT Rules).

### **5. COMPARATIVE LEGAL FRAMEWORKS**

Jurisdictions have responded differently to the proliferation of deepfakes and the way they are being used as weapons in sextortion. While several nations have enacted laws specifically designed to prevent the harmful use of synthetic media, others still rely on antiquated legal systems that are frequently unable to handle the complexity of this changing threat. In terms of controlling deepfakes and safeguarding victims of image-based sexual assault, a comparative study identifies both the finest approaches and enduring weaknesses that exist worldwide.

---

<sup>10</sup> **Budapest Convention on Cybercrime**, Council of Europe, ETS No. 185 (2001)

## **5.1 India: Fragmented Frameworks and Emerging Reforms**

India's legal response to sextortion and deep fakes remains fragmented and reactive. As deep fakes are not explicitly criminalized under existing legislation, victims are forced to navigate a patchwork of legal remedies under the IT Act, 2000, and the Bharatiya Nyaya Sanhita, 2023.

The BNS includes some relevant provisions:

Section 74 – voyeurism

Section 76 – stalking and cyberstalking,

Section 77 – insult to the modesty of a woman,

Section 356 – defamation,

Section 63 – obscenity.

However, these provisions were not formulated with synthetic or AI-generated content in mind, and many require the content to be "real" or "obscene" by traditional legal standards. Deep fake material, which may appear realistic but is wholly fabricated, falls into a legal grey area. Moreover, non-consensual synthetic sexual imagery is not explicitly recognized as a distinct offence under Indian law.

Some positive developments include:

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021<sup>11</sup>, which mandate intermediaries to remove non-consensual nudity or sexual content within 24 hours of a user complaint.

Inclusion of cyberstalking and harassment under Section 76 of BNS, which may apply to some instances of deepfake sextortion.

However, enforcement remains weak due to limited digital literacy among law enforcement, inadequate forensic capacity, and lack of gender-sensitive training. India's non-ratification of the Budapest Convention on Cybercrime also limits international cooperation in pursuing cross-border offenders.

In essence, despite growing awareness, India's existing legal framework is inadequate to deal with the speed, scale, and harm of deep fake-driven sextortion, highlighting the need for urgent legal reform and targeted legislation.

---

<sup>11</sup> **The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021**, Rule 3(2)(b).

## **5.2 United States: Free Speech v/s Targeted Harm**

Attempts to outlaw altered or synthetic speech are complicated by the United States' strong constitutional commitment to freedom of expression under the First Amendment, which shapes legal responses. However, there has been increasing awareness in recent years that deepfakes might violate rights like privacy, autonomy, and reputation when they are used maliciously. A number of jurisdictions have taken the initiative and passed laws specifically targeting deepfakes, especially when it comes to non-consensual pornography.

For example, the deployment of deepfakes for election manipulation or sexual exploitation is illegal in California, Texas, and Virginia. Distributing sexually explicit deepfake photos without consent is prohibited by California law, particularly if done with malicious intent<sup>12</sup>. In a similar vein, victims of the unlawful use of their likeness may file a lawsuit in New York for civil damages. State-by-state variations in these regulations, however, result in a lack of consistency and certain weaknesses when content is transferred between jurisdictions.

Attempts at the federal level have been more circumspect. Despite being presented to Congress in 2019, the DEEPFAKES Accountability Act has not yet been signed into law. A "duty of care" approach, in which platforms would be obligated to proactively regulate and identify altered content, has been promoted by legal professors such as Danielle Citron. The robust protection of free speech and the decentralized structure of U.S. law imply that victim protections remain uneven and insufficient, despite the fact that the U.S. legal system benefits from sophisticated forensic techniques and active civil society engagement.

## **5.3 European Union: A Human Rights-Centric Approach**

In response to deepfakes and digital ills, the European Union takes a more rights-based and regulatory stance. People are entitled to control their personal data, including their appearance and likeness, under the General Data Protection Regulation (GDPR)<sup>13</sup>. Therefore, using personal photos in deepfake material without permission may violate data privacy rights and result in administrative sanctions as well as legal lawsuits. Additionally, big platforms are explicitly required by the EU's Digital Services Act (DSA), which

---

<sup>12</sup> **California Civil Code**, Section 1708.86.

<sup>13</sup> **General Data Protection Regulation**, Regulation (EU) 2016/679.

was enacted in 2022<sup>14</sup>, to identify and eliminate unlawful content, including deepfake pornography. The DSA fortifies user rights to appeal content judgments and requires transparency in algorithmic content curation. This is in line with the EU's larger strategy of using regulatory monitoring rather than just criminal legislation to keep platforms responsible.

National action has also been taken by a number of EU member states. Section 201a of the German criminal code, for instance, makes it illegal to distribute pictures<sup>15</sup> that gravely infringe on someone else's privacy. This also applies to synthetic sexual content. Laws against revenge porn have been introduced in France, and they may soon be extended to include AI-generated content. A more comprehensive legal response to deepfake-related problems is provided by the EU, where, in contrast to the US, freedom of expression is balanced with privacy, dignity, and anti-discrimination norms.

#### **5.4 United Kingdom: Image-Based Abuse and Online Safety**

When it comes to identifying image-based sexual abuse (IBSA) as a separate type of harm, the UK has taken the lead internationally. Retaliation porn and upskirting are illegal under the 2019 Voyeurism (Offences) Act and the Abuse of Trust Offences Act. Crucially, the UK government has recognized the danger of synthetic media, and it is anticipated that the forthcoming Online Safety Act would mandate that platforms address damaging deepfake content. In its 2022 report, the UK Law Commission suggested making it illegal to share and produce sexually explicit deepfakes<sup>16</sup>, even if the pictures are of actual occurrences. Additionally, it demanded that psychological injury from synthetic abuse be legally recognized, particularly in cases where there was no actual sexual action. These changes highlight the need for proactive criminal legislation in addition to platform accountability, and they represent a forward-looking knowledge of how gendered online harms are changing.

#### **5.5 Lessons and Gaps in Global Regulation**

A number of recurring themes show up across different jurisdictions. First, while several nations are making little steps in the right direction, none have yet established a complete legal framework to combat deepfake sextortion. Second, the efficacy of current legislation frequently rests on victims'

---

<sup>14</sup> **Digital Services Act**, European Union (2022)

<sup>15</sup> **German Penal Code**, Section 201a.

<sup>16</sup> **UK Law Commission**, *Intimate Image Abuse: Consultation Report* (2022), available at <https://www.lawcom.gov.uk/project/intimate-image-abuse> (last visited Jul. 31, 2025).

access to justice, which is hampered by obstacles including technical illiteracy, stigma-related anxiety, and insufficient enforcement. Third, most nations function under locally compartmentalized legal systems, which restricts cross-border accountability despite the fact that the global nature of digital platforms necessitates international cooperation.

On the other hand, the UK's image-based abuse reforms and the EU's rights-based framework present encouraging models that India may adopt. In the meanwhile, India's constitutional structure must take into account the conflict between the need to regulate synthetic harms and the right to free speech, as demonstrated by the U.S. experience.

## **6. WAY FORWARD AND POLICY RECOMMENDATIONS**

There is an urgent need for institutional, technological, and legal reform due to the growing threat of deepfakes and their application in sextortion. Like many other nations, India is locked in a race between slow legal growth and quick technology innovation. Even these disjointed regulations provide some protection, synthetic digital abuse's speed, anonymity, and cross-border nature surpass them. In order to prevent abuse and safeguard the constitutional principles of autonomy, privacy, and dignity in the digital realm, a thorough, victim-centered, and forward-looking approach is necessary.

### **6.1 Implement a Comprehensive Law on Digital Sexual Harassment and Deepfakes**

First and foremost, India needs to think about passing a specific rule that makes it illegal to produce, distribute, and possess non-consensual deepfake material, particularly when it involves sexual content. The special harms of synthetic content are not adequately addressed by the present reliance on regular BNS,2023 and IT Act restrictions. Clear definitions of "synthetic media," "manipulated likeness," and "image-based sexual abuse" should be included in any new legislation, with consent serving as the primary legal requirement. This law needs to be technology-neutral, gender-sensitive, and flexible enough to accommodate new AI tools.

In order to differentiate between parody, false information, and deliberate exploitation, the legislation should also incorporate graded punishments according to the degree and intent. The legislation must take into consideration psychological injury even in cases when no "real" substance is used, as inspired by EU and UK revisions. Criminal punishments must be accompanied by civil remedies like damages and injunctive relief.

## **6.2 Fortify the 2021 Information Technology Regulations**

Platforms are currently required by the Intermediary Guidelines and Digital Media Ethics Code Rules, 2021 (often referred to as the IT Rules) to take down any content that contains non-consensual nudity within 24 hours. These clauses must be amended, nevertheless, to specifically cover deepfake and artificial intelligence-generated content. Digital platforms and social media intermediaries must have explicit commitments to proactively identify, categorize, and remove synthetic sexual content using both automated techniques and human moderation.

Furthermore, data on complaints and measures related to deepfake content must be included in platforms' transparency reports. Fast-track grievance redressal procedures ought to be required, particularly in situations involving child abuse and gender-based violence, where promptness is essential to minimizing harm.

## **6.3 Invest In Forensic and Deepfake Detection Skills**

India needs to make investments in developing AI detection tools for the public sector, such to projects like Microsoft's Video Authenticator and the Facebook and MIT-led Deepfake Detection Challenge. Building domestic capacity for forensic verification of digital content—which courts and law enforcement may depend on as expert testimony—requires cooperation with academic institutions and international AI labs.

Additionally, state cybercrime cells and judicial academies ought to establish specialized forensic labs to educate judges, prosecutors, and law enforcement officials on the technical aspects of sextortion and deepfakes. Legal remedies won't be real if we don't have the means to tell the difference between the two.

## **6.4 Establish Awareness Campaigns and A National Register Of Offenders**

In addition to serving as a deterrent, a national register of convicted digital sex offenders might help law enforcement identify repeat offenders. In addition, there needs to be a national awareness campaign to teach young people about consent, internet safety, and reporting procedures, particularly in schools and universities. Given the psychological pain and social stigma that victims—especially women—face, cybercrime reporting portals and One Stop Centres (OSCs) ought to incorporate a counselling and legal aid support system.

In order to enable victims to speak up without feeling ashamed or afraid, collaborations with NGOs, digital literacy groups, and mental health specialists will be essential.

### **6.5 Encourage Global Collaboration and ratify The Budapest Convention**

International cooperation is essential since digital misuse frequently transcends national boundaries. India should give the Budapest Convention on Cybercrime, which allows law enforcement authorities to share evidence and access data across borders, a serious second look. When deepfake servers are hosted overseas or the offenders live outside of Indian jurisdiction, being a part of this framework would allow for quicker action.

In order to promote international ethical standards and treaty commitments on AI misuse, data privacy, and tech business accountability, India can also assume a leading role in multilateral forums such as the G20, BRICS, and the UN Internet Governance Forum.

### **6.6 Reforms in the Courts and Institutions**

The growing negative effects of synthetic media, especially with regard to women's rights and digital privacy, need to be brought to the attention of the Indian judiciary. Courts ought to implement victim-friendly procedures like in-camera hearings and case file sealing for deepfake extortion. Furthermore, much-needed uniformity and clarity would be provided by the Supreme Court or High Courts creating model rules on how to handle cases involving digital sexual assault, including bail considerations, the admissibility of evidence, and victim protection.

The National Cyber Crime Reporting Portal may house a central nodal agency that would act as a specialized authority to handle complaints, start takedown requests, offer forensic assistance, and keep an eye on patterns in the use of deepfakes.

## **7. CONCLUSION**

The emergence of deepfake technology and its usage in sextortion represents a perilous turning point in the digital era, where advances in technology surpass ethical and legal protections and artificial reality is used as a weapon to inflict actual pain. This research has demonstrated that deepfakes are

more than just new technologies or disinformation tools; they pose a serious risk to people's privacy, autonomy, and physical integrity, especially when they are used to mimic non-consensual sexual content.

The absence of a strong and cohesive judicial system in India and around the world puts victims at risk, gives criminals more confidence, and delays justice. Although limited relief is provided by specific sections in the Information Technology Act, the BNS,2023 and court rulings, these laws are reactive, disjointed, and inadequately prepared to handle the unique circumstances of synthetic misuse. Gendered violence, online anonymity, transnational jurisdiction difficulties, and victim stigmatization exacerbate the ethical, legal, and technological challenges surrounding deepfakes and necessitate a coordinated and systematic response.

But there is also a chance because of the crisis. It exhorts lawmakers, civil society, educators, and technologists to rethink digital governance in a way that upholds human dignity without impeding creativity. A digital environment where permission is paramount and harm is confronted with accountability can be established through explicit legislation, enhanced platform accountability, AI-powered detection technologies, judicial and law enforcement capacity building, and strong victim-support mechanisms.

In addition to regulating technology, it is imperative that we foster ethical standards, digital literacy, and a public awareness of the dangers posed by deepfakes as we navigate a more synthetic future. The era of artificial intelligence necessitates a new legal imagination that is agile, rights-oriented, and proactive, much like laws were once modified to accommodate new realities brought about by print, film, and photography. Only then can we start to balance the need to protect human dignity in a digital environment with the enormous potential of AI.

# **NAVIGATING THE DIGITAL CHILDHOOD: REIMAGINING CONSENT, GUARDIANSHIP, AND AUTONOMY IN INDIA'S DATA PROTECTION REGIME FOR CHILDREN**

Ms. Suji Cheriyan\*

---

## **ABSTRACT**

The Digital Personal Data Protection Act, 2023 (DPDPA), introduces significant provisions for protecting children's personal data, establishing 18 years as the age of digital consent and requiring verifiable parental consent for processing minors' data. This article critically examines the intersection of child rights, parental control, and best interest principles within the DPDPA framework. Through doctrinal analysis and case law examination, this study explores the tensions between protecting children from digital exploitation while preserving their evolving autonomy. The research reveals critical gaps in the legislation, particularly concerning the lack of clear guidelines for determining a child's best interests in digital contexts and the absence of mechanisms for children to challenge parental decisions. The article argues for a more nuanced approach that balances protection with recognition of children's developing capacity for autonomous decision-making in the digital realm. It concludes with recommendations for implementation that better align with constitutional principles of child welfare and international best practices in children's rights.

**Keywords:** Digital Personal Data Protection Act, Children's Rights, Parental Consent, Digital Autonomy, Best Interest Principle

---

\* Assistant Professor, Bharata Mata School of Legal Studies, Aluva, MG university, Kottayam

## **1. INTRODUCTION**

The advent of digital technologies has fundamentally transformed how children interact with the world, creating new opportunities for learning, socialization, and self-expression while simultaneously exposing them to unprecedented risks.<sup>1</sup> The Digital Personal Data Protection Act, 2023 (DPDPA) represents India's landmark attempt to regulate personal data processing, with specific provisions addressing the unique vulnerabilities of children in digital spaces.<sup>2</sup>

The DPDPA's approach to children's data protection reflects a complex balancing act between protecting minors from exploitation and recognizing their evolving capacity for autonomous decision-making. By establishing 18 years as the age of digital consent and mandating verifiable parental consent for processing children's data, the Act takes a decidedly protective stance.<sup>3</sup> However, this approach raises fundamental questions about the intersection of child rights, parental authority, and the best interest principle that warrant critical examination.

This article seeks to analyze the DPDPA's provisions concerning children's data protection through the lens of constitutional principles, international human rights standards, and evolving jurisprudence on children's rights. The analysis will explore whether the Act's framework adequately balances protection with autonomy and examine the practical implications of its implementation for various stakeholders.

## **2. THEORETICAL FRAMEWORK: CHILD RIGHTS AND DIGITAL AUTONOMY**

### **2.1. The Evolution of Children's Rights in India**

The recognition of children as rights-bearing individuals rather than mere objects of protection has been a gradual evolution in Indian jurisprudence. The Supreme Court's landmark decision in *Gaurav Jain v. Union of India* established that children possess fundamental rights that must be protected by both the state and society.<sup>4</sup> Subsequently, in *Bachpan Bachao Andolan v. Union of India*, the Court

---

<sup>1</sup> Sonia Livingstone and Julian Sefton-Green, *The Class: Living and Learning in the Digital Age* (New York University Press, 2016) 45-67.

<sup>2</sup> The Digital Personal Data Protection Act, 2023, No. 22 of 2023.

<sup>3</sup> *Ibid.*, s. 9.

<sup>4</sup> *Gaurav Jain v. Union of India*, (1997) 8 SCC 114.

emphasized that the best interest of the child must be the paramount consideration in all decisions affecting children.<sup>5</sup>

The constitutional framework for children's rights finds expression in Article 15(3), which empowers the state to make special provisions for children, and Article 21, which guarantees the right to life and personal liberty.<sup>6</sup> The Supreme Court has consistently interpreted Article 21 to include the right to privacy, as established in *Justice K.S. Puttaswamy (Retd.) v. Union of India*, thereby extending privacy protection to children.<sup>7</sup>

## **2.2 The Concept of Evolving Capacity**

The principle of evolving capacity, recognized in Article 5 of the United Nations Convention on the Rights of the Child (UNCRC), acknowledges that children's capacity to exercise their rights develops progressively with age and maturity.<sup>8</sup> This principle challenges binary approaches to childhood that treat all minors uniformly, instead advocating for a more nuanced understanding that recognizes individual differences in developmental capacity.

In the digital context, evolving capacity becomes particularly relevant as children often demonstrate sophisticated understanding of technology while potentially lacking awareness of long-term consequences of data sharing.<sup>9</sup> The challenge lies in creating legal frameworks that protect children without unnecessarily restricting their legitimate digital participation.

## **3. THE DPDPA FRAMEWORK FOR CHILDREN'S DATA PROTECTION**

### **3.1 Key Provisions and Definitions**

The DPDPA defines a "child" as any individual below the age of 18 years, aligning with the Juvenile Justice (Care and Protection of Children) Act, 2015.<sup>10</sup> Section 9 of the Act specifically addresses the processing of children's personal data, establishing two primary requirements: verifiable parental consent and prohibition of processing that could cause harm to the child.<sup>11</sup>

---

<sup>5</sup> *Bachpan Bachao Andolan v. Union of India*, (2011) 5 SCC 1.

<sup>6</sup> India Const. Arts. 15(3), 21.

<sup>7</sup> *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

<sup>8</sup> Convention on the Rights of the Child, Nov. 20, 1989, 1577 U.N.T.S. 3, art. 5.

<sup>9</sup> Danah Boyd, *It's Complicated: The Social Lives of Networked Teens* (Yale University Press, 2014) 78-95.

<sup>10</sup> The Digital Personal Data Protection Act, 2023, s. 2(c); Juvenile Justice (Care and Protection of Children) Act, 2015, s. 2(12).

<sup>11</sup> The Digital Personal Data Protection Act, 2023, s. 9.

The Act mandates that data fiduciaries must obtain verifiable consent from the parent or lawful guardian before processing a child's personal data.<sup>12</sup> This requirement extends beyond mere notification to parents, demanding affirmative consent that can be verified through reasonable means. The legislation also prohibits tracking, behavioral monitoring, and targeted advertising directed at children.<sup>13</sup>

### **3.2 Enforcement Mechanisms and Penalties**

The DPDPA establishes the Data Protection Board of India with powers to investigate violations and impose penalties.<sup>14</sup> Violations of children's data protection provisions attract monetary penalties up to ₹250 crores, reflecting the legislature's intent to create strong deterrents against misuse of children's data.<sup>15</sup>

The Act also provides for blocking of non-compliant platforms and services, giving the enforcement authority significant powers to protect children's digital rights.<sup>16</sup> However, the practical implementation of these mechanisms remains to be tested through actual enforcement actions.

## **4. CRITICAL ANALYSIS OF THE CONSENT FRAMEWORK**

### **4.1 The Parental Consent Paradigm**

The DPDPA's reliance on parental consent as the primary protection mechanism for children reflects a traditional understanding of childhood that prioritizes protection over participation. While this approach aligns with established legal principles regarding parental authority, it raises several concerns in the digital context.

First, the requirement for verifiable parental consent may create barriers to children's legitimate digital participation. Educational platforms, social networking sites, and other digital services that could benefit children may become less accessible due to compliance costs and technical challenges in implementing robust consent verification systems.<sup>17</sup>

---

<sup>12</sup> *Ibid.*, s. 9(1).

<sup>13</sup> *Ibid.*, s. 9(2).

<sup>14</sup> *Ibid.*, s. 18.

<sup>15</sup> *Ibid.*, s. 33.

<sup>16</sup> *Ibid.*, s. 20.

<sup>17</sup> Centre for Internet and Society, "Age Verification and Parental Consent: Technical and Policy Challenges" (2023) 12 *Digital Rights Quarterly* 34-56.

Second, the consent framework assumes that parents are best positioned to make decisions about their children's digital participation. However, research suggests that many parents lack understanding of digital technologies and their implications, potentially leading to uninformed consent decisions.<sup>18</sup> The Supreme Court's observation in *Shilpa Sailesh v. Varun Sreenivasan* regarding the importance of informed decision-making becomes particularly relevant in this context.<sup>19</sup>

#### **4.2 Limitations of the Consent Model**

The consent-based approach fails to account for situations where parental interests may conflict with the child's best interests. The Bombay High Court's decision in *Vandana Sitalaxmi Shah v. State of Maharashtra* recognized that parental rights are not absolute and must be exercised in the child's best interest.<sup>20</sup> However, the DPDPA provides no mechanism for children to challenge parental consent decisions or for independent assessment of whether such decisions serve the child's best interests.

Furthermore, the binary nature of consent (granted or withheld) does not accommodate the nuanced reality of children's digital engagement. A 17-year-old seeking to participate in online educational programs or social advocacy may have legitimate interests that conflict with parental preferences, yet the current framework provides no avenue for recognizing such autonomy.

### **5. THE BEST INTEREST PRINCIPLE IN DIGITAL CONTEXTS**

#### **5.1 Constitutional and International Obligations**

The best interest principle, enshrined in Article 3 of the UNCRC and recognized by Indian courts as a fundamental consideration in child-related matters, requires that all decisions affecting children prioritize their welfare.<sup>21</sup> The Supreme Court in *Laxmi Kant Pandey v. Union of India* established that the best interest standard must guide all child protection measures.<sup>22</sup>

In digital contexts, determining a child's best interest requires balancing immediate protection needs against long-term developmental interests, including the right to information, expression, and participation in digital society. The Delhi High Court's reasoning in *Baby Manji Yamada v. Union of*

---

<sup>18</sup> Monica Bulger et al., "Digital Parenting: How Parents Perceive and Manage Technology Use" (2017) 34 *New Media & Society* 2237-2256.

<sup>19</sup> *Shilpa Sailesh v. Varun Sreenivasan*, (2023) 4 SCC 394.

<sup>20</sup> *Vandana Sitalaxmi Shah v. State of Maharashtra*, 2020 SCC OnLine Bom 2847.

<sup>21</sup> Convention on the Rights of the Child, *supra* note 8, art. 3.

<sup>22</sup> *Laxmi Kant Pandey v. Union of India*, (1984) 2 SCC 244.

*India* regarding the multifaceted nature of children's best interests provides useful guidance for digital contexts.<sup>23</sup>

## **5.2 Challenges in Implementation**

The DPDPA's failure to provide clear criteria for determining children's best interests in digital contexts creates implementation challenges. Unlike traditional child protection scenarios where physical welfare is paramount, digital contexts involve complex trade-offs between privacy, autonomy, education, and social participation.

The lack of guidance on how data fiduciaries should assess whether their services serve children's best interests creates uncertainty and may lead to overly restrictive approaches that limit children's beneficial digital engagement. The Madras High Court's emphasis in *R. Bommi v. Union of India* on the need for clear standards in child protection matters highlights this deficiency.<sup>24</sup>

## **6. COMPARATIVE ANALYSIS AND INTERNATIONAL BEST PRACTICES**

### **6.1 European Union's Approach**

The European Union's General Data Protection Regulation (GDPR) provides a more nuanced approach to children's data protection by setting the age of consent at 16 years (with member states having discretion to lower it to 13) and recognizing different standards for different types of data processing.<sup>25</sup> The GDPR also explicitly recognizes children's right to be forgotten and provides mechanisms for children to withdraw consent independently.<sup>26</sup>

The European approach acknowledges that older children may have legitimate interests in making independent decisions about their digital participation, particularly in educational and social contexts. This recognition of evolving capacity provides a more flexible framework than the DPDPA's uniform approach.

---

<sup>23</sup> *Baby Manji Yamada v. Union of India*, (2008) 13 SCC 518.

<sup>24</sup> *R. Bommi v. Union of India*, 2011 SCC OnLine Mad 5632.

<sup>25</sup> General Data Protection Regulation, Regulation 2016/679, art. 8.

<sup>26</sup> *Ibid.*, art. 17.

## **6.2 Lessons from Other Jurisdictions**

The United Kingdom's Age Appropriate Design Code provides detailed guidance on how digital services should be designed to protect children while supporting their development and well-being.<sup>27</sup> This approach focuses on creating inherently protective digital environments rather than relying solely on consent mechanisms.

California's California Consumer Privacy Act includes provisions for children's data protection that recognize different levels of protection for different age groups, reflecting a more nuanced understanding of developmental capacity.<sup>28</sup> These examples suggest alternative approaches that could inform implementation of the DPDPA.

## **7. PRACTICAL IMPLICATIONS AND IMPLEMENTATION CHALLENGES**

### **7.1 Technology and Verification Challenges**

The requirement for verifiable parental consent presents significant technical challenges. Current age verification technologies are often unreliable, raising questions about their effectiveness in protecting children while potentially creating privacy risks for adults.<sup>29</sup> The Supreme Court's concerns about technological overreach in Aadhaar cases provide relevant context for evaluating these verification requirements.<sup>30</sup>

Moreover, the global nature of digital services complicates enforcement of Indian consent requirements. Multinational platforms may struggle to implement India-specific age verification systems, potentially leading to service restrictions that affect children's digital access.

### **7.2 Educational and Social Implications**

The DPDPA's restrictions may have unintended consequences for children's education and social development. Educational technology platforms, which have become increasingly important especially post-COVID-19, may face compliance challenges that affect their accessibility to

---

<sup>27</sup> UK Information Commissioner's Office, Age Appropriate Design Code (2020).

<sup>28</sup> California Consumer Privacy Act, Cal. Civ. Code S. 1798.120.

<sup>29</sup> Priya Kumar et al., "No Telling Passersby, the Internet is Broken: Age Verification and Online Age Assurance" (2021) Proceedings of the CHI Conference on Human Factors in Computing Systems 1-15.

<sup>30</sup> *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2018) 1 SCC 1.

children.<sup>31</sup> The Supreme Court's recognition in *Anuradha Bhasin v. Union of India* of the importance of internet access for educational purposes becomes relevant in this context.<sup>32</sup>

Social media platforms and communication services that facilitate peer interaction and social development may also be affected, potentially limiting children's opportunities for digital socialization and civic participation.

## **8. RECOMMENDATIONS FOR REFORM AND IMPLEMENTATION**

### **8.1 Age-Graduated Approach**

The DPDPA could benefit from an age-graduated approach that recognizes different levels of capacity at different developmental stages. Children above 16 years, for instance, might be permitted to provide consent for certain types of low-risk data processing, particularly in educational contexts, while maintaining parental consent requirements for high-risk processing.

This approach would align with the evolving capacity principle and provide a more nuanced framework that balances protection with autonomy. The Supreme Court's recognition in *Mohini Jain v. State of Karnataka* of the importance of educational access could support such differentiated treatment.<sup>33</sup>

### **8.2 Best Interest Assessment Framework**

Implementation of the DPDPA should be accompanied by clear guidelines for assessing children's best interests in digital contexts. These guidelines should consider factors such as educational benefit, developmental appropriateness, privacy risks, and the child's own expressed preferences where age-appropriate.

---

<sup>31</sup> UNESCO, "Education: From Disruption to Recovery" (2023), available at <https://en.unesco.org/covid19/educationresponse>.

<sup>32</sup> *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637.

<sup>33</sup> *Mohini Jain v. State of Karnataka*, (1992) 3 SCC 666.

An independent mechanism for reviewing disputed cases, similar to child welfare committees established under the Juvenile Justice Act, could provide oversight and ensure that the best interest principle is meaningfully applied.<sup>34</sup>

### **8.3 Child-Friendly Complaint Mechanisms**

The Act should be supplemented with accessible complaint mechanisms that allow children to raise concerns about data processing or to seek review of parental consent decisions in appropriate circumstances. The National Commission for Protection of Child Rights could potentially play a role in developing such mechanisms.<sup>35</sup>

## **9. CONCLUSION**

The DPDPA represents a significant step forward in protecting children's digital rights, but its current framework reveals tensions between protection and autonomy that require careful navigation. While the Act's protective approach is commendable, its rigid consent requirements and lack of recognition for children's evolving capacity may inadvertently limit beneficial digital participation. The challenge lies in creating a framework that protects children from genuine harms while recognizing their developing autonomy and legitimate interests in digital participation. This requires moving beyond binary approaches to consent and developing more nuanced mechanisms that can assess and protect children's best interests in specific contexts.

Future implementation of the DPDPA should draw upon constitutional principles of child welfare, international best practices, and empirical research on children's digital capabilities and needs. Only through such a comprehensive approach can India create a digital protection framework that truly serves children's best interests while preparing them for responsible digital citizenship.

The ultimate goal must be to create digital environments that are inherently safe for children while supporting their development, learning, and social participation. This requires collaboration between lawmakers, technology companies, educators, parents, and children themselves to develop solutions that balance protection with empowerment in the digital age.

---

<sup>34</sup> Juvenile Justice (Care and Protection of Children) Act, 2015, s. 27.

<sup>35</sup> Commission for Protection of Child Rights Act, 2005, s. 13.

**INDIA'S JUVENILE JUSTICE SYSTEM:  
BRIDGING THE GAP BETWEEN LEGISLATIVE  
INTENT AND IMPLEMENTATION REALITY**

Shalini Shukla \*

---

**ABSTRACT**

This research examines the evolution of India's juvenile justice system, tracing its transformation from traditional welfare-oriented approaches to contemporary rights-based frameworks. The study analyses how India's system has historically oscillated between rehabilitation and punishment, influenced by colonial interventions, international conventions, and domestic social pressures. Beginning with ancient Hindu and Islamic legal traditions that recognized children's diminished responsibility, the paper traces the system's development through British colonial reforms, including the Apprentices Act of 1850 and the Reformatory Schools Act of 1876. These early interventions established the foundation for specialized treatment of juvenile offenders, emphasizing reformation over punishment. Post-independence legislation, particularly the Juvenile Justice Acts of 1986, 2000, and 2015, reflects India's gradual adoption of international standards, including the UN Convention on the Rights of the Child and Beijing Rules. However, the 2015 Act marks a controversial shift by allowing juveniles aged 16-18 to be tried as adults for heinous crimes, representing a departure from purely rehabilitative principles. The research reveals a significant gap between progressive legislative frameworks and practical implementation. Despite having comprehensive laws, India's juvenile justice system is only impressive on paper but ineffective in practice. The paper concludes by recommending specialized judicial training, dedicated juvenile justice officers with longer tenures, and reorienting juvenile courts as child development facilitators rather than punitive institutions.

**Keywords:** *Juvenile Justice, Rehabilitation, Child Rights, Legal Reform, Reintegration;*

---

\* Research Scholar, Dr. Ram Manohar Lohia National Law University, Lucknow

## **INTRODUCTION**

I am the child. All the world waits for my coming. All the earth watches with interest to see what I shall become. Civilization hangs in the balance, for what I am, the world of tomorrow will be. I am the Child. You hold in your hand my destiny. You determine, largely, whether I shall succeed or fail. Give me, I pray you, those things that make for happiness. Train me, I beg you, that I may be a blessing to the world.

The above quote from Mamie Gene Cole's book *The Child's Appeal* perfectly captures the responsibility that society bears towards its youngest members, equating the child not merely as individual but as the living embodiment of a civilization's future. This verse serves as a moral compass for any discourse on child welfare, by reminding the policymakers, legal reformers and societies at large, that success or failure of a child is shaped entirely by – adequate training, protection and empowering the child. It is this very recognition that has, over a period of time, compelled nations to formulate these moral obligations into formal regulations incorporating both welfare and rights of children. When compared to how human rights have changed since the 17th century around the world, the recognition of child rights has come a little later.

The term juvenile justice stems from the Latin term *juvenis* meaning young, referring to a justice system tailored for youth offenders. This concept arose from the belief that issues of juvenile delinquency in abnormal situations could not be adequately addressed through the traditional criminal law framework meant for adults.<sup>1</sup> Over time, the juvenile justice system has evolved beyond simply addressing young offenders' needs to include specialized preventive treatment services. It now incorporates community support mechanisms and strives to balance formal state interventions with community, family and institutional approaches. This comprehensive system focuses on prevention, rehabilitation, and socialization of children through various channels including schools and religious bodies.<sup>2</sup>

The juvenile justice system in India has its origins rooted in the colonial era under British rule. The introduction of separate legal mechanisms and institutions to address juvenile delinquency was a direct consequence of Western ideas and developments in the fields of prison reform and juvenile

---

<sup>1</sup> VED KUMARI, *THE JUVENILE JUSTICE SYSTEM IN INDIA: FROM WELFARE TO RIGHTS* 44 (2<sup>nd</sup> ed. 2010).

<sup>2</sup> U.N. Secretariat of The Sixth United Nations Congress on Prevention of Crime and Treatment of Offenders, Working Paper on Juvenile Justice: Before and After the Onset of Juvenile Delinquency, U.N. Doc. A/CONF.87/5 (June 4, 1980).

justice.<sup>3</sup> However, the changes adopted in India to deal with delinquent juveniles were not merely replications of practices implemented in England.

While the juvenile court established under the Madras Children Act of 1920<sup>4</sup> reflected the same approach as the English Children Act of 1908,<sup>5</sup> subsequent legislations shifted from this model. Indian laws dispensed with the presence of lawyers, aligning more closely with the *parens patriae* philosophy of the American juvenile courts. Moreover, the concept of juvenile welfare boards, originating in Scandinavian countries, became an integral component of Indian laws pertaining to delinquent and neglected children from the 1960s onward.

The evolution of the juvenile justice system in India was influenced by a multitude of factors, both domestic and international. The area of the child welfare has always taken back seat in India and making them the “second-class-citizens” in the sense that the welfare policies were always made from the perspective of adult members of the society.<sup>6</sup> It witnessed a gradual shift from a ‘welfare’ approach to a ‘rights-based’ perspective, accompanied by significant structural changes in the criminal justice system. This reform process was shaped by the pioneering efforts of several nations to implement juvenile justice concepts effectively.

This research paper aims to trace the historical development of the juvenile justice system in India, exploring its conceptual foundations and the factors that have influenced its progression.

## **CONCEPTUAL DEVELOPMENT OF JUVENILE JUSTICE**

Throughout history, societies have recognized the need to treat young offenders differently from adults. This distinction dates back over 4,000 years to ancient legal codes like Hammurabi’s, which addressed runaways, children who disowned their parents and sons who cursed their fathers.<sup>7</sup> About 2,000 years ago, both Roman civil law and church law established different treatment for juveniles based on their age and responsibility level. Ancient Jewish legal traditions in the Talmud limited punishments for young people, prohibiting corporal punishment before puberty (defined as age 12 for girls and 13 for boys) and exempting those under 20 from capital punishment. Similarly, Muslim legal

---

<sup>3</sup> *Id.*

<sup>4</sup> Madras Children Act, 1920 (Act 4 of 1920).

<sup>5</sup> The Children Act, 1908 (8 Edw. 7. c. 67).

<sup>6</sup> Elizabeth Scott, *The Legal Construction of Adolescence*, 29 HARV. L. REV. 547 (2000).

<sup>7</sup> STEVEN M. COX *et. al.*, JUVENILE JUSTICE: A GUIDE TO THEORY, POLICY AND PRACTICE (9th ed. 2018).

traditions showed leniency toward young offenders, typically not applying the death penalty to those under 17 years of age.

The juvenile justice system in Western nations has undergone a significant conceptual evolution over time. The early roots can be traced back to the recognition that children, due to their developmental immaturity, cannot be considered as culpable or criminally responsible as adults for unlawful actions and that children are unique and require specific treatment throughout their formative years.<sup>8</sup> This sparked initial reforms segregating juvenile and adult offenders in prisons and improving conditions for incarcerated youth.

By the mid-1800s in Britain, disruptive youth behaviour was widely recognized as a social concern requiring public attention. While formal juvenile courts weren't established until 1908, the country had already developed a system of reformatories and industrial schools by the 1850s. These institutions operated on the principle that young offenders could be effectively resocialized through specific interventions. The reformatory approach believed that removing children from negative influences, teaching them to read and write, providing religious guidance, training them in practical work skills, and motivating them to follow rules would transform them into law-abiding citizens.<sup>9</sup> This early approach laid the groundwork for more formalized juvenile justice systems and reflected the emerging understanding that children required different treatment than adult offenders. These reformatories, refuges and correctional institutions prioritized custody over any meaningful rehabilitative efforts. This inertia, coupled with an alarming spike in juvenile crime rates, required a fundamental rethinking of how to approach this issue.

Two key guiding principles emerged regarding the best way to establish a separate system for dealing with juvenile offenders, shaping its foundational philosophy. The first was the English model based on the principle of segregating juveniles from adult offender populations. This gave rise to the juvenile courts established under the 1908 Children's Act. However, these remained criminal courts in nature, simply maintaining separate spaces and procedures for trying youth.

---

<sup>8</sup> Richard C. Mitchell, *Reflections on the UNCRC's Future from a Transdisciplinary Bricoleur*, 21 INT'L J. CHILD. RTS. 510 (2013).

<sup>9</sup> Reformatories in Victorian England worked by putting criminals into different groups, giving them a chance to improve their position in the system. These places controlled not just working-class children and those seen as dangerous, but also homeless kids who had no families except their friends. Middle-class Victorians saw these street children almost like stray animals. Colonial thinking affected how people viewed these children, which is why they were often called "savages" and "arabs."

The underlying notion was that juveniles were still delinquents or wrongdoers, just requiring some modifications to the regular criminal procedure rather than an entirely distinct approach. Dispositions were based on offense severity and public safety factors, much like the adult criminal justice system.

In contrast, the American juvenile courts were based on the *parens patriae* doctrine - the state essentially assuming a paternalistic guardian role making decisions in the best interests of the child, akin to a parent (in loco parentis). The state had supreme authority over these juveniles and the courts were not criminal in nature, following an entirely separate non-punitive process centered on the juvenile's welfare and rehabilitation.

In the late 1800s, reformers advocated for a unified approach to children under 14, arguing that distinctions between paupers, vagrants, and criminal children were unnecessary. They believed neglected children were at risk of becoming paupers or criminals, leading to the development of *parens patriae*, where the government intervenes to prevent future criminality.<sup>10</sup>

The Scandinavian countries adopted yet another alternative model inspired by the *parens patriae* principle - a juvenile welfare board system rather than formal courts. The reasons for this divergence from the court system are unclear and appear to have emerged independently.

While juvenile welfare boards took root in Norway from 1896, it was the establishment of the pioneering juvenile court in Cook County, Illinois in 1898 that influenced the rapid spread of the court model across the United States and then globally over the subsequent decades. Though the motivations and socio-political forces driving this dissemination are not well-documented historically.

Initially in the U.S., the *parens patriae* doctrine was implemented in an expansive manner, granting the state broad discretionary authority over juveniles in their presumed best interests and welfare. However, this faced criticism as investigations into juvenile facilities exposed rampant abuse, harsh conditions and neglect that seemed to contradict the nurturing premise of the doctrine. The landmark 1967 U.S. Supreme Court case *In Re Gault*<sup>11</sup> proved to be a pivotal turning point in this transition. The Court recognized that rather than being nurtured, juveniles in the system had "suffered the worst

---

<sup>10</sup> Sanford J. Fox, *Juvenile Justice Reform: An Historical Perspective*, 22 STAN. L. REV. 1187 (1970).

<sup>11</sup> 387 U.S. I (967).

of both worlds” - lacking the procedural rights adults had and also deprived of the care they were entitled to under the *parens patriae* premise.

*Gault* case established that juveniles facing potential institutionalization in delinquency proceedings must be afforded due process protections like adequate notice, opportunity for counsel, protection against self-incrimination and confronting accusers. However, rather than wholly abandoning the ‘welfare’ rehabilitative model, efforts were made to strike a balance preserving both components - ensuring juvenile’s rights through fair processes while still prioritizing their best interests and providing opportunities for positive youth development wherever possible.

The United Nations approach also underwent this evolution over time. The initial 1959 Declaration on the Rights of the Child prioritized providing appropriate treatment, education and care for children with special needs - more aligned with the ‘welfare’ model. However, the 1985 UN Standard Minimum Rules (hereinafter referred as Beijing Rules) shifted to emphasizing accountability, due process and procedural safeguards in dealing with juvenile offenders, while still promoting their overall welfare.

This culminated in the seminal 1989 Convention on the Rights of the Child, which aimed to harmonize the ‘welfare’ and ‘rights’ considerations. It recognized children’s rights to due process but also made their best interests<sup>12</sup> the preeminent priority in all state actions concerning them. Other key principles included giving weight to children’s views, non-discrimination, family care, and progressively realizing their economic and social rights.

Subsequently 1990 Riyadh Guidelines<sup>13</sup> further reinforced the importance of upholding juvenile rights and well-being through minimum intervention and providing developmental opportunities for at-risk youth within the wider human rights framework.

Across nations, juvenile justice models exist along a spectrum - some adhering more closely to a child protection approach treating delinquency as an aberration and focusing on education and social services. Others gravitate towards a crime control model that views juveniles as culpable for their actions and emphasizes punishment and accountability.

---

<sup>12</sup> Convention on the Rights of the Child, art. 3, Nov. 20, 1989, 1577 U.N.T.S. 3.

<sup>13</sup> U.N. Guidelines for the Prevention of Juvenile Delinquency (The Riyadh Guidelines), G.A. Res. 45/112, U.N. Doc. A/RES/45/112 (Dec. 14, 1990).

Ultimately, the conceptual evolution has been towards a synthesized approach - incorporating robust procedural rights and constitutional protections for juveniles as safeguards against potential excess state action. However, this coexists with maintaining a primary focus on juveniles' rehabilitation, welfare, and positive youth development through the state's paternalistic guidance and investment in prevention policies. Rather than completely discarding one model for the other, modern juvenile justice policy and practice aims to harmonize protecting juveniles due process rights with pursuing the most positive long-term outcomes for their growth into productive citizens through evidence-based services, diversion, and minimum intervention where appropriate.

## **HISTORY OF JUVENILE JUSTICE IN INDIA**

By the mid-nineteenth century, the issue of disorderly children had become a recognized public problem in Britain. While juvenile courts were not established until 1908, a network of reformatories and industrial schools was already in place by the 1850s. These institutions operated on the belief that juvenile offenders could be rehabilitated through proper socialization, which included removal from negative influences, basic education, religious instruction, work training, and fostering obedience. George Behlmer emphasized that the Victorian approach to correction relied heavily on careful classification, giving offenders a chance to determine their bureaucratic class. This emerging disciplinary system targeted working-class children, homeless children, and those from the "dangerous classes," viewing them similarly to stray animals. The language of colonialism influenced this metropolitan concern, with street children often referred to as "savages" and "Arabs," a discourse that mirrored colonial views of Indians.

In India, however, the implementation of these British reformative models faced significant challenges. Unlike in Britain, where specialists ran juvenile institutions, Indian reformatories were often supervised by military doctors and jailors without specialized training. Colonial officials believed that medical knowledge could help determine the ages and treatment needs of Indian juveniles. The superintendents of juvenile wards were typically career jailors, and their superiors had even less experience with juvenile delinquency. Despite a willingness to experiment with European techniques, the lack of expertise and inconsistent commitment to modern

rehabilitation methods underscored the makeshift nature of the colonial reformatory system.<sup>14</sup>

Colonial modernity further complicated the ideal of reform and rehabilitation in India. The need to maintain racial distinctions between the British and Indians made the ideological placement of reformed criminals problematic. Deep-seated beliefs in the incorrigibility of certain Indian subgroups, particularly those convicted of property crimes, led to debates about whether children from these groups should be admitted to reformatories. Some colonial observers saw these children as suitable for institutionalization, essential for preventing the resurgence of criminal activities like thuggee. Others, however, viewed them as unreformable and corrupting influences, preferring to exclude them from reformatories.

The scope of juvenile delinquency in India was both broader and narrower than in Britain. While British delinquency was primarily urban, Indian delinquents came from both urban and rural areas. Over time, urban delinquents became more prominent in the colonial consciousness, with cities like Calcutta, Madras, and Rangoon embodying anxieties about population control. Urban delinquency, similar to that depicted in the works of Charles Dickens and Mary Carpenter, was seen as a class issue, with children either from broken families or so impoverished that they had never experienced proper parental control. The state aimed to replace absent parents in these urban contexts. In contrast, rural delinquency was viewed through a lens of racial and cultural exoticism, with British observers believing that rural Indian children were criminal because of their control by criminal adults. These children often came from “wild” groups, with their criminal convictions reflecting their social identities rather than specific acts.

The British discourse on delinquency included female children, seen either as victims of male lust or agents of sexual corruption. In the 1880s, concerns about child prostitution in London led to various legal and institutional measures to address female delinquency. In India, however, juvenile delinquents were overwhelmingly boys. While girl criminals were not invisible, they were rarely admitted to reformatories, reflecting concerns about their marriage prospects and societal norms. These girls faced diverse punishments, ranging from short prison terms to life in penal transportation or confinement in lunatic asylums.<sup>15</sup> Some were even sent to the Andaman Islands, where they were

---

<sup>14</sup> Satadru Sen, *A Separate Punishment: Juvenile Offenders in Colonial India*, 63 J. ASIAN STUD. 83 (2004).

<sup>15</sup> *Id.*

encouraged to marry male convicts.<sup>16</sup> Despite pressure from evangelical activists for female reformatories, girls were notably excluded from Reformatory Schools Acts, except in Madras. This exclusion was justified by concerns that native opinion would not accept girls being institutionalized under male supervision at marriageable ages. Most colonial administrators believed that rehabilitation for Indian girls meant marriage, fearing that incarceration would harm their marital prospects on the mainland. Incarceration was seen as detrimental to Indian girl's futures, with rehabilitation often equated to marriage rather than institutional reform.

India's juvenile justice system has strong historical connections to Western developments, particularly drawing from European and American advancements in children's rights and human rights jurisprudence. The system's formal beginnings can be traced to the Apprentices Act of 1850, which established the first legal framework specifically addressing juvenile offenders in India.

During British colonial administration, several key pieces of legislation progressively shaped India's approach to young offenders. The Whipping Act of 1864 implemented corporal punishment as a deterrent, while both the Indian Penal Code (1860) and Criminal Procedure Code (1861) recognized children's unique status by establishing separate legal procedures for them. The Reformatory Schools Act of 1876 further developed institutional responses, followed by the Borstal School Act and the Children's Act of 1918. Various regions also enacted their own legislation, such as the Bengal and Madras Children's Acts, which specifically addressed neglected and delinquent children.

These legal developments collectively reflected a gradual shift toward rehabilitation rather than pure punishment. The British colonial approach increasingly emphasized reforming young offenders through specialized institutions rather than simply imposing punitive measures,<sup>17</sup> establishing foundations that would influence India's post-independence juvenile justice framework.

India's juvenile justice system evolved significantly following the influential recommendations of the Indian Jail Committee (1919-1920). This committee explicitly advocated for differential treatment between child and adult offenders, opposing child imprisonment and promoting reformatory schools and specialized children's courts with flexible, informal procedures.

---

<sup>16</sup> *Id.*

<sup>17</sup> *Id.*

Notably, the Committee also emphasized preventive measures, suggesting special provisions for children who hadn't yet committed crimes but were at risk due to adverse environments or lack of proper guardianship. These recommendations led to important legislative changes, including the addition of Section 29B to the Criminal Procedure Code of 1898, establishing separate trials for offenders under 15 years old.

These reforms triggered a wave of provincial legislation beginning with the Madras Children Act (1920), followed by similar acts in West Bengal (1922) and Bombay (1924). However, these regional laws lacked uniformity, particularly regarding age definitions, with male children variously defined between 14-16 years and female children between 16-18 years.<sup>18</sup>

An important turning point came when juvenile justice was transferred from the State List to the Concurrent List in India's Constitution, enabling the central government to create standardized national legislation. This led to the Juvenile Justice Act of 1986 and its successor, the Juvenile Justice (Care and Protection of Children) Act of 2000. During this legislative evolution, the distinct category of "adolescent" disappeared, creating a binary system where individuals under 18 were legally classified as children, while those 18 and older were treated as adults.

India's juvenile justice system can be better understood by examining its development through five distinct historical periods, each representing significant shifts in approach and philosophy.

### **Status of juveniles prior to 1773**

India's historical approach to juvenile justice has deep roots in its traditional legal systems. Both Hindu law (Manusmriti) and Islamic law (Sharia) emphasized child welfare, making parents primarily responsible for children's care and protection, with community support when families couldn't provide adequately.<sup>19</sup> These systems recognized children's diminished responsibility. Hindu law prescribed cleaning duties rather than fines for children who littered public roads, while Islamic law specifically prohibited executing children. These provisions demonstrate an early understanding that children required special consideration and weren't fully accountable for their actions. So, the Indian

---

<sup>18</sup> B. B. Pande, *In the Name of Delhi Gang Rape: The Proposed Tough Juvenile Justice Law Reform Initiative*, 2 J. NAT'L L. U. DELHI 152 (2014).

<sup>19</sup> VED KUMARI, WELFARE TO RIGHTS, *supra* note 2 at 4.

culture historically treated child as a child in need of care and protection such that if he has committed any wrong, he was treated not as per the adult's law.<sup>20</sup>

### **Status of juveniles from 1773 – 1849**

The colonial period from 1773-1849 marked the beginning of formalized juvenile welfare systems in India. As the East India Company and later the British government dominated India, social reforms gained momentum. Colonial economic policies damaged the agrarian economy, forcing many into urban slums and increasing child destitution and delinquency.<sup>21</sup> In response, prominent Indians like Krishna Chandra Ghoshal and Jai Narayan Ghoshal advocated for establishing homes for destitute juveniles in Calcutta. The first school for vagrant and orphaned children opened in Bombay in 1843 (later renamed the David Sason Industrial School), focusing on reforming child offenders through apprenticeships and industrial training rather than punishment.

### **Period from 1850 – 1919**

Between 1850-1919, specific juvenile legislation emerged. The Apprentices Act of 1850, India's first law providing special status for juveniles required vagrant children and minor offenders aged 10-18 to serve sentences as apprentices<sup>22</sup>, redirecting them from criminal influences toward productive skills, making them able to earn a living.<sup>23</sup> The Indian Penal Code of 1860 established age-based criminal culpability through the concepts of *doli incapax* and *doli capax* (Sections 82-83), protecting children from prosecution until they could understand their actions. The Criminal Procedure Code of 1898 mandated separate trials for those under 15 and confinement in reformatories rather than adult prisons, shifting from punishment to reformation.

Despite these reforms, the Whipping Act of 1864 came with a troubling setback. Responding to increasing juvenile crime rates (particularly in Poona, where cases rose from one to sixty-five between 1860-1861), authorities chose corporal punishment over investing in reformatories, a decision driven more by economic considerations than rehabilitation principles. Between 1872-1875, however, the Poona juvenile prison demonstrated success through education and aftercare.

---

<sup>20</sup> Vaidehi Joshi, *Juvenile Delinquency and Evolution of Juvenile Justice in India*, 3 INT'L J. L. MGMT. & HUMAN. 686 (2020).

<sup>21</sup> Erika Rickard, *Paying Lip Service to the Silenced Juvenile Justice in India*, 21 HARV. HUM. RTS. J. (2008).

<sup>22</sup> Act XIX of 1850 allowed magistrates and justices of the peace to "apprentice" children between the ages of ten and eighteen to private "masters," who might put them to work and discipline them physically.

<sup>23</sup> Ashley Blackburn, *The Juvenile Justice System in India: From Welfare to Rights*, 3 YOUTH VIOLENCE & JUV. JUST. 395 (2005).

The Reformatory Schools Act of 1876 further distinguished juvenile treatment, placing boys under 15 in reformatories rather than prisons, with incarceration periods of 3-7 years. Its 1897 successor focused specifically on treatment and rehabilitation for children aged 7-15, though notably excluding girls. The Criminal Tribes Amendment Act of 1897 established special schools for children of designated “criminal tribe” members aged 4-18. The Criminal Procedure Code of 1898 extended reformatory confinement until age 18, followed by probation until 21.<sup>24</sup>

This evolution reflects India’s gradual development of a juvenile justice philosophy that prioritized rehabilitation over punishment, recognizing children’s unique developmental needs and diminished culpability.

### **Period from 1919 – 1950**

From 1919-1950, India’s juvenile justice system underwent significant transformation. The Indian Jail Committee (1919-1920) recommended separate treatment for child offenders, opposing their imprisonment, and advocating for reformatory schools and specialized children’s courts with flexible procedures. The Committee also prioritized prevention for at-risk children living in harmful environments or without proper guardianship.

This initiated a wave of provincial legislation beginning with the Madras Children Act (1920), which thoughtfully categorized young people as “child” (under 14), “young person” (14-18), and “youthful offender” (under 18 with convictions) rather than using the term delinquent.<sup>25</sup>

Similar legislation followed with the Bengal Children Act (1922), though Bengal had operated juvenile courts since 1914 and the Bombay Children Act (1924). The 1940s saw further expansion with children’s acts in Delhi (1941), Mysore (1943), Travancore (1945), Cochin (1946), and East Punjab (1946).<sup>26</sup>

The Vagrancy Act of 1943 extended protection to vulnerable children under 14 who were begging, lacked guardianship, had parents involved in criminal activities or substance abuse, or were otherwise

---

<sup>24</sup> Tapan Chakraborty, *Delinquency and Juvenile Justice System in India*, in John A. Winterdyk, *The Juvenile Justice System: International Perspective* (2002).

<sup>25</sup> CLAYTON A. HARTJEN & SESHU KETHINENI, *COMPARATIVE DELINQUENCY: INDIA AND THE UNITED STATES* 36 (1996).

<sup>26</sup> S.K. Bhattacharyya, *Juvenile Justice System in India*, 23 *J. INDIAN L. INST.* 608 (1981).

at risk.<sup>27</sup> Throughout this period, international influences like League of Nations declarations helped shape India's increasingly rehabilitation-focused approach to juvenile justice.

### **Post 1950**

The foundation of India's juvenile justice system was established in the post-independence era when the country adopted its Constitution. The Preamble established guiding principles of justice, liberty, and equality that informed subsequent juvenile justice legislation. Special need was felt for specifically recognizing the need to protect vulnerable sections of society, including children, by allowing for special provisions in their Favor.<sup>28</sup>

This constitutional framework represented an important ideological shift from colonial-era regulations to a system seeking to foster an egalitarian society with justice at its center. The constitutional promise to secure "social, economic, and political" justice extended to children in conflict with law, establishing state responsibility for their protection and rehabilitation. The Constitution's promise of social justice materialized statutorily after a decade of its coming into force, through the Children Act of 1960<sup>29</sup>, marking the first comprehensive legislation addressing child welfare and juvenile delinquency. This Act incorporated essential elements of *care, welfare, maintenance, training, education, and rehabilitation for neglected and delinquent children....*<sup>30</sup> However, its limited applicability left many children subject to disparate state-level frameworks, creating inconsistency in juvenile justice administration.

The 1980s witnessed substantial transformation in juvenile justice globally. Following India's ratification of the Beijing Rules, the Juvenile Justice Act of 1986 was enacted. This legislation established formal institutional mechanisms - Juvenile Justice Boards (hereinafter referred as JJBs) and Juvenile Courts - for adjudicating cases involving juvenile offenders. Magistrates were granted primary implementation authority and considerable discretionary powers concerning children in conflict with law.<sup>31</sup> Despite these structural improvements, the system struggled to fully realize its rehabilitative ideals.

---

<sup>27</sup> Bengal Vagrancy Act, 1943 (India).

<sup>28</sup> India. Const. art. 15(3).

<sup>29</sup> Children Act, No. 60 of 1960 (India) (repealed).

<sup>30</sup> *Id.*, preamble.

<sup>31</sup> Juvenile Justice Act, No. 53 of 1986, § 18 (India) (repealed).

Further evolution occurred following the adoption of the United Nations Convention on the Rights of the Child in 1989.<sup>32</sup> The Juvenile Justice Act of 2000 (hereinafter referred as the 2000 Act), emerged from these international principles, focusing on rehabilitating children into mainstream society while protecting their interests during delinquency proceedings. This legislation consolidated laws relating to juveniles in conflict with law and children requiring care and protection, embracing a rights-based approach to juvenile justice. This law focused on the rights-based approach towards children *while consolidating and amending the law relating to juveniles in conflict with law and children in need of care and protection*.<sup>33</sup> However, with the advent of time, this legislation faced challenges both from outside the judiciary and within the judiciary to bring a change in the juvenile justice system.<sup>34</sup> The 2000 Act formed the foundation for The Juvenile Justice (Care and Protection of Children) Act, 2015 (hereinafter referred as the 2015 Act), with many provisions carried forward.

The primary motivation behind these challenges was societal protection against juvenile offenders, with a clear intent to make the juvenile justice system more stringent and aggressive. These challenges did not go unheard and finally paved the way for coming into force of the 2015 Act.

### **THE 2015 ACT AND THE FLAWS**

This legislation was influenced by international developments including the Beijing Rules, the Convention on the Rights of the Child (1989), and the UN Rules for the Protection of Juveniles Deprived of their Liberty (1990). The 2015 Act, while incorporating many provisions from the 2000 Act, it introduced controversial innovations, particularly regarding the treatment of juveniles between 16-18 years accused of “heinous” crimes.

Parliamentary debates leading to this legislation reveal that concerns about “heinous offenses committed by children” were a primary motivation. These debates focused disproportionately on the age of criminality rather than comprehensive juvenile welfare. This shift reflects a move from a welfare-oriented system to one with more punitive formulations. The 2015 Act allows for juveniles aged 16-18 to be treated as adults for heinous crimes following assessment, representing a significant shift from previous approaches that maintained uniform treatment for all under 18.

---

<sup>32</sup> Convention on the Rights of the Child, G.A. Res. 44/25, U.N. Doc. A/RES/44/25 (Nov. 20, 1989).

<sup>33</sup> Ved Kumari, *Quagmire of Age Issues under the Juvenile Justice Act: From Inclusion to Exclusion*, (2)51 JILI 163 (2009).

<sup>34</sup> B.B. Pande, *‘Bad’ Juveniles and the ‘Worst’ Juvenile Justice Law? The Second Challenge to Juvenile Justice Law in Darga Ram v. State of Rajasthan*, 57(1) JILI (2015).

The 2015 Act is a well-intentioned legislative framework that nonetheless suffers from many practical constraints. It assigns the JJBs an excessively broad mandate to protect children throughout their interaction with the juvenile justice system,<sup>35</sup> effectively transforming the JJB from an adjudicative body into an oversight mechanism with unrealistic responsibilities. This overextension is similarly evident in Section 19, which burdens Children's Courts with rehabilitative follow-up duties despite the Principal Magistrate's limited time and significant case backlogs. These provisions reflect a fundamental disconnect between legislative idealism and implementation realities, creating a system that appears comprehensive in theory but proves ineffective in practice.

The Act further complicates matters by placing judges in a position of unresolvable tension between criminal adjudication and child protection roles. These judicial officers, predominantly trained in criminal jurisprudence rather than child welfare principles, struggle to reconcile these competing responsibilities. The underlying challenge stems not from inherent institutional deficiencies but from the attempted integration of divergent objectives: punitive justice, rehabilitation, and societal reintegration.<sup>36</sup> Rather than addressing these tensions, the 2015 Act codifies them, resulting in onerous institutional responsibilities that render the law more symbolic than substantive.<sup>37</sup> This gap between legislative aspiration and practical implementation undermines the efficacy of juvenile justice in India and calls into question whether the system genuinely serves the best interests of children in conflict with the law.

The juvenile justice system originated from principles of liberal criminal justice<sup>38</sup>, with the understanding that juvenile minds are not mature enough to form the intent required for criminal culpability.<sup>39</sup> However, over time, juvenile courts have evolved to incorporate both reformatory and punitive elements, creating inherent contradictions. These two aspects are sometimes referred to as diversionary and interventionist justifications for juvenile courts.<sup>40</sup> The diversionary principle aims to divert juveniles from the adult criminal justice system, while the interventionist principle focuses

---

<sup>35</sup> The Juvenile Justice (Care and Protection of Children Act), 2015, section 8(3).

<sup>36</sup> Aayush Raj, *JUVENILE JUSTICE SYSTEM IN INDIA: Incoherence of Principles, Cutbacks, And Judges' Dilemmas*, 3 SHIMLA L. REV. 94 (2020).

<sup>37</sup> *Id.*

<sup>38</sup> *Id.*

<sup>39</sup> Gauri Pillai & Shrikrishna Upadhyaya, *Juvenile Maturity and Heinous Crimes: A Re-look at Juvenile Justice Policy in India*, 10 NUJS L. REV. 49 (2017).

<sup>40</sup> *Supra* note 35.

on rehabilitation through social intervention. Indian juvenile justice institutions have struggled to effectively implement either principle.

The judgement of apex court in the case of *Sampurna Behura v. Union of India*<sup>41</sup> highlights the apathy of the juvenile justice system, showing the miserable condition and lack of resources both in human capital and infrastructure. The court conjointly read the Integrated Child Protection Scheme (ICPS), the J.J. Act of 2000, and the J.J. Act of 2015, effectively assessed the system's condition, and revealed the ineffectiveness of the existing scheme and the significant loopholes in its implementation.

The Act endows the State with responsibility for implementing child protection measures, but evidence suggests significant lapses in fulfilling these obligations. Children who interact with the juvenile justice system often remain outside the safety net of protection and holistic development that the legislation envisions.

The 2015 Act's differential treatment of children aged 16-18 years involved in heinous crimes, presents another dilemma. While the Act ostensibly upholds the "best interest of the child" principle, it simultaneously creates mechanisms to treat these adolescents as adults, especially when children accused of serious offenses to be tried in regular courts rather than before the specialized JJB. This provision fails on three critical counts: *it reclassifies adolescents as adults based solely on offense severity, it subjects them to courts not bound by juvenile justice principles, and it prioritizes societal interests over the child's rehabilitation needs.*<sup>42</sup> This represents not merely a procedural shift but departure from the rehabilitative foundations of juvenile justice.

The Supreme Court in 2012, in, *Ashwani Kumar Saxena vs State of Madhya Pradesh*<sup>43</sup> overruled the decisions of lower court's decision, wherein, the Chief Judicial Magistrate (CJM) and the First Additional Sessions Judge, both, rejected documentary evidence of Juvenile's age (school records and birth certificates), relying instead on bone ossification tests to declare him an adult offender. The Supreme Court held that the CJM and First Additional Sessions Judge had fundamentally misunderstood the Juvenile Justice Act provisions regarding age determination. This case exposes a troubling reality: the accused lost five years of his life to procedural errors and misinterpretation of

---

<sup>41</sup> 2018 (4) SCC 433.

<sup>42</sup> *Supra* note 35.

<sup>43</sup> 2012 (9) SCC 750.

juvenile justice laws. This raises serious questions about whether a system claiming to prioritize rehabilitation and the “best interest of the child” actually fulfils these principles in practice.

## **WAY FORWARD**

India’s juvenile justice system needs to bridge the gap between its progressive legislative intent and its disappointing practical realities. The 2015 Act established an impressive rights-based framework on paper, but cases like *Ashwani Kumar Saxena* reveal how systemic incompetencies lead to serious miscarriages of justice affecting vulnerable children. These failures stem not from isolated interpretive errors but from lack of understanding regarding the distinctive nature of juvenile proceedings, where child-centric interpretations should be the rule rather than the exception.

Effective implementation demands substantial investment in comprehensive, continuous training programs for judicial officers and other stakeholders. Creating institutional partnerships between state agencies and reputable legal education institutions would help develop specialized curricula addressing both procedural requirements and the psycho-social dimensions of juvenile justice.

The fundamental role conflict facing judges, torn between being adjudicators and protectors, requires establishing a dedicated cadre of judicial officers with specialized expertise and fixed longer tenures. This would address the current problem of frequent transfers that create a perpetual state of inexperience and reinforce inappropriate application of adult criminal justice standards. Specialized judges could develop comprehensive understanding of juvenile matters, ensuring that rehabilitation remains the central focus.

Ultimately, juvenile courts must be reoriented as facilitators of child development rather than punitive institutions. They should serve as gateways to appropriate rehabilitative interventions while protecting children’s rights throughout the process. Despite its progressive legislative evolution from welfare to rights, India’s juvenile justice system remains a “toothless tiger” impressive in statutory formulation but ineffectual in practice. True reform requires not further legislation but reimagined implementation mechanisms, training frameworks, resource allocation, and institutional structures that genuinely advance children’s rights while facilitating their rehabilitation and reintegration into society.

## THE TELECOM ACT, 2023: A FUTURE-READY FRAMEWORK OR A CONSTITUTIONAL REGRESSION

Charupragya Ksuhwaha\*

---

### ABSTRACT

The legal frameworks governing telecommunications assume greater constitutional significance as digital communication continues to shape social interaction, economic activity, and democratic participation. By superseding colonial laws such as the Indian Telegraph Act of 1885 and the Indian Wireless Telegraphy Act of 1933, the Telecommunications Act of 2023 is an all-encompassing legislative effort to modernize India's telecom system. The Act raises significant constitutional and regulatory issues, even though its goal is to establish a technology-neutral regulatory framework capable of handling cutting-edge innovations such as 5G, artificial intelligence, and the Internet of Things. Notably, its broad definition of "telecommunication services" may make it harder to distinguish between infrastructure providers and application-layer services by extending regulatory oversight to over-the-top (OTT) platforms, encrypted messaging services, and digital communication applications. The Act gives the executive broad discretionary authority over internet shutdowns, traffic data collection, biometric verification, and interception, frequently without independent oversight or clear procedural safeguards. Given the constitutional guarantees of privacy, freedom of expression, and due process found in Articles 19 and 21, these provisions warrant careful consideration. Therefore, the Act requires careful evaluation to ensure that regulatory modernization does not undermine democratic accountability, civil liberties, and constitutional governance.

### Introduction

The Telecom Act, 2023, is not just an act of legislative modernization, an act of technological transformation, but operates as a deep re-constitution of the relationship between the state, the market, and the citizen within India in the digital-constitutional understanding.<sup>1</sup> Formulated under a backdrop of greater reliance on the use of digital technology and subsequent increased state engagement in the sphere of cyber-infrastructure spawned by the pandemic, the Act is positioned as a replacement of the colonial Indian Telegraph Act, 1885, and other similar laws. However, the deeper thrust to this

---

\* 4<sup>th</sup> year Student, Dr. Ram Manohar Lohia National Law University

<sup>1</sup> Usha Ramanathan, "Digital Constitutionalism in India," (2020) 57(3) Economic and Political Weekly 17.

statutory reformation is a rebalancing of state sovereign management of digital infrastructure that involves the strong-arm expansion of executive power, the creation of a discretionary power-shadow under which the individual rights of persons of height privilege and power are also undermined in the cause of the national good.<sup>2</sup>

As the internet becomes the prime arena through which civil liberties, speech, associations, and means of livelihood are exercised, the infrastructure of legal frameworks takes on strong constitutional importance. The Telecom Act, 2023 conflates prior separations in the categories of carriage and content by the possible extension of over-the-top (OTT) platforms, encrypted messaging services, and cloud communications into the definition of the Telecommunication services. By so doing, it takes a risk of regulatory trespass, not to mention jurisdictional fog-up in violation of the theory of legal certainty that is indispensable as part of the rule of law.

The equally alarming aspect of the surveillance, suspension, and service denial architecture included in the Act is that such notions as a public emergency and public safety are left widely open and unspecified. The Act grants the Union executive wide-ranging powers to intercept, suspend, or shut down telecom services without clear procedural safeguards, raising fundamental questions about proportionality, necessity, and judicial oversight, particularly in light of judicial pronouncements in *Puttaswamy* and *Anuradha Bhasin*<sup>3</sup>

### **Overview of The Telecommunications Act, 2023**

The Telecommunications Act, 2023 is a game-changer in how India regulated telecom, signing off on the outdated colonialist laws that were scattered all over and instead implementing a new single legal framework that would be modern and ready to tackle the future. It replaces the Indian Telegraph Act, 1885, the Indian Wireless Telegraphy Act 1933 and it modifies the Telecom Regulatory Authority of India (TRAI) Act, 1997 partially. The new law is believed to rationalize and modernize the telecom regulation environment in India in the context of radical changes in technology involving the upcoming 5G, the Internet of Things (IoT), artificial intelligence, and related convergence between telecommunicating and digital service.

---

<sup>2</sup> Rahul Matthan, "Delegated Legislation and Executive Overreach in the Telecom Act," Mint (15 Jan 2024) <https://www.livemint.com/opinion/online-views/the-telecom-bill-makes-a-bold-attempt-to-revise-regulation-for-the-better-11703002587290.html>(accessed 31 July 2025).

<sup>3</sup> *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1; *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637.

The hub of the Act is a wide-ranging definition of telecommunication services that is technology neutral. As opposed to the past laws that only focused on the unique technologies bearing the law such as the telegraph or the wireless communication, the 2023 Act has a wide range of focus on the services involved such as machine to machine (M2M) communication, over-the-top (OTT) communication service, satellite based services, or any other future services facilitating the telecommunication. Such a broad jurisdiction allows the possibility of applying regulations on such web-based applications as WhatsApp, Signal and Telegram that hitherto had been in a legal gray area. The addition of OTT services has revived the issues that surround overregulation, discouragement of innovation, and the chilling effect on user privacy and end-to-end encryption.

This Act also provides for civil penalties and executive-based adjudication instead of judicial oversight, creating apprehension about institutional independence and fair process. Moreover, the efforts by TRAI seem to be severely limited, since most of the recommendatory and regulatory authority that the organization had will be absorbed into the executive.

The Act facilitates ease of infrastructure deployment by offering new, redesigned Right of Way (RoW) provisions. It requires that the approvals for installations of telecom infrastructure are made within one stipulated period under normal terms and conditions. This is intended to mitigate bureaucracy in the implementation of 5G and fiber networks at the urban and rural locations. Moreover, the law introduces a "deemed approval" mechanism, ensuring that applications are automatically considered approved if not acted upon within a stipulated period thereby addressing long-standing concerns of red tape and project delays.

The Act grants large amounts of authority to the executive, especially the Central Government, who now has the ability to grant licenses, assign spectrum (including administrative assignment of spectrum to operate in the interest of the general public), intercept communications, and discontinue services on the basis of public emergency, and national security. Though the justification is that this will prevent national security threats and rationalize the regulation process, opponents say that it is an anomaly without judicial oversight; and the broad discretionary powers will risk mass surveillance and/or loss of constitutional guarantees.

Overall, although the Telecommunications Act, 2023 aims to contemporise the telecom regulatory environment in India, it also provokes complicated discussions regarding surveillance, independence of regulators, digital rights, and the rule of law in a digital democracy.

## **Legal and Regulatory Concerns Arising from the 2023 Act**

### **A) Overbroad Definition of Telecommunication Services**

The Act defines and incorporates a broad definition of the term telecommunication services as found under Section 2(21) of the Act<sup>4</sup>, which includes any service that facilitates the transmission, emission, or reception of messages. Although purportedly presented as technology-neutral and future-friendly, such a definition can subject a vast number of digital media platforms, such as Over-The-Top (OTT) providers, like WhatsApp, Signal, Zoom, and Telegram, to the same regulatory scheme as the legacy telecom providers.

Such an overreach establishes regulatory uncertainty, especially because there is no differentiation between infrastructure providers and application-layer services. Any attempt to regulate such platforms through an undefined and elastic term like "telecommunication services" could fall foul of Article 19(1)(a)<sup>5</sup> of the Constitution, which guarantees the right to freedom of speech and expression. This applies especially where the definition is capable of being used to impose liability with respect to content moderation, service limitation, or authorizing the interception upon generic reasons such as 'public safety' or 'national interest' reasons. This concern resonates with the precedent set in *Shreya Singhal v. Union of India*, where the Supreme Court struck down provisions that were overly broad and infringed on free expression.<sup>6</sup>

Moreover, the OTT services neither use spectrum nor deal with the physical infrastructure of telecom facilities, and thus, the inclusion of OTT in the telecom licenses is doubtful. Sustaining the ability to formulate specific guidelines enables the government to subsequently require content control, pressure on any type of connection interception, or compel decryption of these services, and that poses grave constitutional issues regarding the subjects concerning liberty of communication and secrecy.

### **B) Surveillance and Interception without Judicial Oversight**

---

<sup>4</sup> Government of India, *The Telecommunications Act*, No. 44 of 2023, s 2(21).

<sup>5</sup> Constitution of India, art. 19(1)(a).

<sup>6</sup> *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.

The Telecommunications Act, 2023, significantly enhances the government's powers of surveillance. Sections 20 and 21 of the Telecommunications Act, 2023<sup>7</sup> contain extremely broad powers given to the Central Government to intercept or detail, or suspend telecommunication services in the case of a public emergency or in the name of public safety as well as in the interest of the country, national security, sovereignty, or integrity of India. This is comparable to broad powers that were present in the Indian Telegraph Act, but the institutionalization of such an intrusive tool, without any judicial check (of which there must be one, or there is no statutory legal purity), is very problematic, in a constitutional sense.

The Act does not imply prior judicial authorization, and an independent oversight mechanism is not provided. This is contrary to the international standards. In the case of *Big Brother Watch v UK*,<sup>8</sup> European Court of Human Rights has held that interception regimes lacking safeguards contravenes of Article 8 of the ECHR. The absence of judicial oversight, user notification, or independent authorization mechanisms undermines safeguards mandated by the Supreme Court in *PUCL v. Union of India*<sup>9</sup>, which emphasized necessity, proportionality, and administrative accountability.

#### C) Traffic Data Collection and Metadata Surveillance

Section 22(2) of the Telecommunications Act, 2023 grants the government wide powers to collect and analyze "traffic data", defined to include information related to the routing, time, duration, and type of communication transmitted through telecommunication networks. Such metadata may not necessarily include the content of the communication, but it can still be used to disclose extremely sensitive information about the person, behaviour patterns, social connections, and history of location.

The issues are based on the fact that there are no statutory restrictions on the use of such information. The Act contains no description of purpose limitation, data minimization, retention and deletion systems, and does not put forward any threshold of necessity or proportionality. In the absence of any clear limitations, the provision facilitates the design of the infrastructure that, in turn, allows running mass profiling and tracking real-time behaviour patterns. Further, the country does not have a viable data protection authority that has the potential to audit such collection or prevent abuse.<sup>10</sup>

---

<sup>7</sup> Government of India, *The Telecommunications Act*, No. 44 of 2023, ss 20–21.

<sup>8</sup> *Big Brother Watch and Others v. United Kingdom*, [2021] ECHR 58170/13.

<sup>9</sup> *People's Union for Civil Liberties (PUCL) v. Union of India*, (1997) 1 SCC 301.

<sup>10</sup> Udbhav Tiwari, "India's New Telecom Bill May Threaten End-to-End Encryption" (2023) Mozilla Foundation Blog <https://foundation.mozilla.org> accessed 28 July 2025.

Informational privacy has been legally recognised by global jurisprudence as being comprised of metadata. The Court of Justice of the European Union overturned blanket metadata retention statutes in *Digital Rights Ireland v Minister for Communications* on the grounds that they could not guarantee both targeted and proportionate surveillance.<sup>11</sup> Likewise, the India Supreme Court in *Puttaswamy v Union of India* held that any violation of privacy must fulfill the conditions of legality, necessity, and proportionality.<sup>12</sup> The text of Section 22(2) in its current form fails to meet the above constitutional protections, and threatens to become a vehicle to allow the executive to aggregate data without check, to the detriment of the Constitutionally-enshrined right to privacy under Article 21.<sup>13</sup>

#### D) Threat to End-to-End Encryption

The other important issue in the Telecom Act, 2023 is its effect on end-to-end encrypted communication. Though the term encryption is not directly mentioned in the Act, the wide wording of the term telecommunication services and the licensing mechanism can be applied to OTT communication applications and platforms (e.g. WhatsApp, Signal, and Telegram), which offer the same features as e-mail and voice calls. By extending the telecom regulatory net to these platforms, they may either be forced into decryption, or provide data about the originators of messages, or even construct backdoors providing lawful access.

India does not have a consistent Encryption Policy to bring about a balance between digital rights and maintaining national security. Earlier efforts to frame such a policy in 2015 were rescinded due to backlash against the terms of invasiveness.<sup>14</sup> The fact that the 2023 Act is silent in regards to encryption-related protections creates a significant degree of regulatory confusion. This ambiguity can have a thawing effect on all speech and prevent users, activists, journalists, lawyers, and general people with millions of users of these secure content distribution sites from trusting their digital infrastructure.

#### E) Executive Rule-Making and Delegated Legislation

One of the greatest challenges in the Telecommunications Act, 2023, is its unwarranted delegation of legislative powers to the executive, in this regard, mostly the Department of Telecommunications

---

<sup>11</sup> *Digital Rights Ireland v. Minister for Communications*, Case C-293/12, Court of Justice of the European Union (2014).

<sup>12</sup> *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.

<sup>13</sup> Constitution of India, art. 21.

<sup>14</sup> Ministry of Communications and IT, *Draft National Encryption Policy*, 2015 (withdrawn), <https://www.meity.gov.in> accessed 31 July 2025.

(DoT). Numerous substantive provisions expressly introduced as Skeleton Clauses are core statutory provisions dealing with areas like licensing, surveillance, interception, and management of traffic data with substantive detail to be specified by means of delegated rule-making.

In *In re Delhi Laws Act* the Supreme Court ruled that conditional legislation and delegated rule-making contribute to the rule of modern governance but that delegation ceases to be constitutional where de facto principle gives way to where fundamental aspects of the legislature are abdicated by the executive.<sup>15</sup> An example of the problem demonstrated in the Telecom Act are Sections 3, 20, 21 and 22 which grant broad discretion and fail to impose any restriction limiting thresholds, procedural safeguards, or mechanisms of accountability.<sup>16</sup>

#### F) Biometric-Based Subscriber Verification

Section 3(7) of the Act makes it possible that the government may require verification of the identity of telecom users using biometrics, which brings about new concerns related to privacy, consent, and exclusion.<sup>17</sup> This exception permits authorized parties to amass biometric information without a system to afford those subject to these systems the choice of means of identification, alternative ID-based systems, or prevention of unauthorized use.

This practice is directly contrary to the ideas put forward in the case of Justice K.S. Puttaswamy , where the apex court held the mandatory one in Aadhaar-SIM as unconstitutional on the grounds of failing the three-fold test of proportionality under Article 21. The Court has noted that such data collection should be legally grounded, should be legitimate, and should have minimal interference. The Telecom Act does not give any clarification on what would be a legitimate aim to justify, or how biometric data is imperative in curbing SIM-related fraud.

#### G) Internet Shutdowns and Access Restrictions

As per section 20(2) of the Act, the Government can suspend telecommunication services due to any public emergency, or due to public safety & the government has the power to do so, either by the Central Government or the Government of any State.<sup>18</sup> Though this is in line with Rule 2(1)<sup>19</sup> of the

---

<sup>15</sup> *In re Delhi Laws Act*, AIR 1951 SC 332.

<sup>16</sup> *The Telecommunications Act*, No. 44 of 2023, ss 3, 20, 21, 22.

<sup>17</sup> *The Telecommunications Act*, No. 44 of 2023, s 3(7).

<sup>18</sup> *The Telecommunications Act*, No. 44 of 2023, s 20(2).

<sup>19</sup> Rule 2(1), *Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules*, 2017, notified under s 7 of the Indian Telegraph Act, 1885.

Temporary Suspension of Telecom Services Rules, 2017, there is a lack of internalization of the safeguards that were prescribed in the Supreme Court judgment *Anuradha Bhasin v Union of India*<sup>20</sup>.

In *Anuradha Bhasin*, the Court mentioned that the restriction imposed on the internet access should be of limited duration, should be proportionate, and should be reviewable by a court. Notably, the Court declared that shutdown orders should be publicly announced, reviewed at regular intervals, and should not be permanent. Although these directions are explicit, the Telecom Act is not clear on transparency of the procedures, it does not impose a time limit on shutdowns, and it does not specify that any order should be published and read before an independent committee.

India remains the world leader in internet shutdowns, and vague justifications such as a need to maintain healthy public order, or to control rumours, are repeated. Failing to enshrine the *Anuradha Bhasin* protections into the Telecom Act will be the equivalent of making arbitrary suspensions of digital connectivity an institution. Since internet access to fundamental rights like free expression, education, health, and economic participation is paramount to rights, the lack of procedural guarantees in Section 20(2) means that the democratic functioning and constitutional freedoms are at stake.

#### H) Spectrum Allocation Discretion

The Act provides the Central Government with broad licensing, interception and spectrum assignment authority in the interests of the spectrum to be utilized publicly on a case by case basis on matters of Public interest. Nevertheless, the phrase of public purpose has not been clearly defined leading to the fear that the discretion can be used to escape the auctioning regime which was held to be compulsory by Supreme Court in 2G Spectrum Case.<sup>21</sup>

Furthermore, the Act places the Telecom Regulatory Authority of India (TRAI) on the periphery of major decisions that affect the spectrum assignment and licensing duties, undermining the dissimilar control. When compared to regulatory schemes in UK (Ofcom) or the US (FCC), where quasi-judicial autonomy has ensured transparency in the market by removing some sense of the politicization of the

---

<sup>20</sup> *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637.

<sup>21</sup> *Centre for Public Interest Litigation v. Union of India*, (2012) 3 SCC 1.

market, DoT based governance in India is doubly vulnerable to criticism of enabling politicization of the market and of providing a move towards the lack of checking and balance in the market system.<sup>22</sup>

### **Recommendations and Reform Proposals**

The current Telecommunications Act, 2023 should also be adjusted and modified in such a way that it would correspond to the constitutional values, individual rights, and would bring clarity to the regulations. To start with, the definition of telecommunication services can be changed in such a way that any Over-the-Top (OTT) service is explicitly not covered, except where such exception is justified. Trying to regulate messaging applications and content-based applications in the same way as traditional telecom providers can become excessive and pose certain threats to net neutrality.

Second, the surveillance intrusions that are authorized under the Act, especially the interception of data and ending of the service, should be open to judicial scrutiny. Procedural safeguards embedded in the Act i.e. prior approval of an independent body, approvals with time limits and review of approvals made will help ensure that the Act becomes consistent with the standards of *PUCL v Union of India* and *Puttaswamy v Union of India*.

Third, checks and balances within the institutions are negated by the marginalization of TRAI. This independence of the regulatory authority in licensing, allocation of spectrum, and in settling disputes should be restored to improve transparency and accountability.

Fourth, collection of traffic data and metadata in 22(2) must be subjected to narrow purpose limitation, minimization principles, and an evident data storing period. Finally, biometric identification should be voluntary with the support of strong data protection standards. Any delegated legislation impacting fundamental rights should undergo parliamentary scrutiny to ensure democratic legitimacy.

### **Conclusion**

The Telecommunications Act 2023 is a revolutionary legal measure that strives to update and streamline the telecommunications infrastructure in India. Its generality of definition, the power it gives to the executive to exercise its powers, and the absence of procedural protections present a serious problem of challenges to constitutional values. This lack of strong checks and balances,

---

<sup>22</sup> Peter Lunt and Sonia Livingstone, *Media Regulation: Governance and the Interests of Citizens and Consumers* (SAGE Publications 2012) 34–37.

particularly in the areas of surveillance, licensing, and the shutting down of the internet, has the potential to compromise the right to privacy, the right to freedom of expression, and the right to due process. The digital infrastructure increasingly becomes part of our lives, and being civically engaged in a democratic society, it is necessary to make sure that the regulatory framework of such a diverse sphere is aligned with the principles of accountability, proportionality, and transparency, consistent with the constitutional arrangements for governance in the digital age.

# **A CRITICAL EVALUATION OF THE COMPETITION (AMENDMENT) ACT, 2023**

Dr. Isha Wadhwa Sharma\*

---

## **ABSTRACT**

The Competition (Amendment) Act, 2023, has ushered in significant substantive and procedural changes to the competition law framework in India and is the most comprehensive amendment to the Competition Act, 2002, to date. In this paper, the author critically analyses the amendments made to the Competition Act, 2002, by the Competition (Amendment) Act, 2023. This paper analyses specifically the amendments to provisions relating to anti-competitive agreements, regulation of combinations, procedure followed by the CCI, penalty on global turnover, and leniency. It further analyses the newly inserted provisions regarding settlement and commitment. It also highlights the other amendments, such as the power of CCI to issue guidelines, limitation period, changes in the definition of Relevant Product Market, pre-deposit of penalty in case of appeal, and decriminalization of certain offences. In the conclusion, the author highlights significant issues not addressed in the Competition (Amendment) Act, 2023.

## **I. Introduction**

Competition law has been growing at a rapid pace due to the ever-changing business model and economic behaviour across the world. In India, the Competition Act, 2002, repealed the Monopolies and Restrictive Trade Practices Act, 1969, and there was a shift from curbing monopolies to promoting competition. The Preamble of the Competition Act, 2002 provides for multiple goals, including establishing the Commission to prevent practices having an adverse effect on competition, to promote and sustain competition, to ensure freedom of trade, and lastly to protect the interests of consumers.

The Competition Act, 2002, was amended thrice before the 2023 amendment. In 2007, amendments were made to change the composition of the Competition Commission of India (CCI), and the Competition Appellate Tribunal (COMPAT) was established to hear the appeals against the decision of the CCI. In 2009, the amendment transferred all the cases related to restricted trade practices pending before the MRTP Commission to the CCI. Lastly, in 2017, the Finance Act abolished the COMPAT, and its powers under the Competition Act, 2002, were

---

\* Assistant Professor, Law centre-II, University of Delhi

transferred to the National Company Law Appellate Tribunal (NCLAT). These three amendments did not change the substantive provisions of the Competition Act, 2002.

In 2011, the then government constituted a High-level Committee under the Chairmanship of Shri Dhanendra Kumar to examine the Competition Act, 2002. The said Committee submitted its report in February 2012, and based on the recommendations in the report, the government introduced the Competition (Amendment) Bill, 2012<sup>1</sup> in Lok Sabha on December 10, 2012. However, the bill was referred to the Standing Committee on December 21, 2012. The Committee submitted its report<sup>2</sup> on February 13, 2014. However, no amended bill was introduced in the Lok Sabha.

On October 1, 2018, the Ministry of Corporate Affairs constituted the Competition Law Review Committee (referred to as 'CLRC') to comprehensively review the competition law framework given the changing business environment and to ensure that the Act integrates strong economic fundamentals. Accordingly, the CLRC submitted its report on July 26, 2019, recommending extensive amendments to the Competition Act, 2002.<sup>3</sup> Premised on the recommendations of the CLRC, the government published the Draft Competition (Amendment) Bill, 2020, on February 12, 2020, for public consultation. However, the draft bill was never introduced in the Lok Sabha.

The Competition (Amendment) Bill, 2022,<sup>4</sup> was introduced in Lok Sabha on August 5, 2022. However, the same was referred to a Joint Parliamentary Standing Committee on Finance (referred to as 'SCF') on August 16, 2022, for analysis and consultation with stakeholders. The Committee presented the report with recommendations<sup>5</sup> to the Lok Sabha on December 13, 2022. After consideration of the report, the Ministry of Corporate Affairs introduced modifications in the 2022 Bill on February 8, 2023, and brought forth the Competition (Amendment) Bill, 2023.

The Competition (Amendment) Bill, 2023, was passed by the Lok Sabha and Rajya Sabha on March 29, 2023, and April 3, 2023, respectively, and it received the assent of the President on

---

<sup>1</sup> The Competition (Amendment) Bill, 2012, *available at*: [https://prsindia.org/files/bills\\_acts/bills\\_parliament/2012/The\\_Competition\\_\(A\)\\_Bill,\\_2012.pdf](https://prsindia.org/files/bills_acts/bills_parliament/2012/The_Competition_(A)_Bill,_2012.pdf). (last visited on June 10, 2025).

<sup>2</sup> Standing Committee on Finance, "Eighty-Third Report: The Competition (Amendment) Bill, 2012 (February, 2014), *available at*: [https://prsindia.org/files/bills\\_acts/bills\\_parliament/2012/SCR-Competition\\_\(A\)\\_Bill.pdf](https://prsindia.org/files/bills_acts/bills_parliament/2012/SCR-Competition_(A)_Bill.pdf). (last visited on June 10, 2025).

<sup>3</sup> Ministry of Corporate Affairs, "Report of Competition Law Review Committee" (July, 2019), *available at*: <https://www.ies.gov.in/pdfs/Report-Competition-CLRC.pdf>. (last visited on June 10, 2025).

<sup>4</sup> The Competition (Amendment) Bill, 2022, *available at*: [https://prsindia.org/files/bills\\_acts/bills\\_parliament/2022/Competition%20\(Amendment\)%20Bill,%202022.pdf](https://prsindia.org/files/bills_acts/bills_parliament/2022/Competition%20(Amendment)%20Bill,%202022.pdf). (last visited on June 10, 2025).

<sup>5</sup> Standing Committee on Finance, "Fifty-Second Report: The Competition (Amendment) Bill, 2022" (December, 2022), *available at*: [https://prsindia.org/files/bills\\_acts/bills\\_parliament/2022/SC%20Report\\_Competition%20\(A\)%20Bill,%202022.pdf](https://prsindia.org/files/bills_acts/bills_parliament/2022/SC%20Report_Competition%20(A)%20Bill,%202022.pdf). (last visited in June 10, 2025).

April 11, 2023. Significant changes were proposed by the Competition (Amendment) Act, 2023 (referred to as ‘Amendment Act, 2023’). As per section 1 of the Amendment Act, 2023, it shall come into force on the date notified by the Central Government, and different dates may be appointed for different provisions. The provisions of the Amendment Act, 2023, have been notified on various dates, May 18, 2023,<sup>6</sup> July 18, 2023,<sup>7</sup> October 26, 2023,<sup>8</sup> February 19, 2024,<sup>9</sup> March 5, 2024,<sup>10</sup> September 9, 2024,<sup>11</sup> and September 19, 2024.<sup>12</sup> This paper critically analyses the key changes introduced by the Amendment Act, 2023, and highlights issues not incorporated by the amendment.

## **II. Key Changes**

The Amendment Act, 2023, has brought many crucial changes in the existing framework under the Competition Act, 2002, which will have significant implications on the competition dynamics in India. The key changes are as follows:

### **Anti-Competitive Agreements (Section 3)**

Significant amendments have been introduced in section 3 of the act. Majorly, the amendment has given specific recognition to the hub and spoke cartel. Further, there are changes in the definition of a tie-in arrangement and an exclusive dealing agreement. Also, in the intellectual property rights exception clause, a general exception clause has been added for any law related to protecting intellectual property rights.

#### **Hub and Spoke Cartel**

A proviso has been added to section 3(3) by the amendment which provides that, “Provided further that an enterprise or association of enterprises or a person or association of persons though not engaged in identical or similar trade shall also be presumed to be part of the agreement under this sub-section if it actively participates in the furtherance of such agreement.”

---

<sup>6</sup> Ministry of Corporate Affairs, *Notification* S.O. 2228(E) (May 18, 2023), available at: <https://www.cci.gov.in/legal-framework/notifications/details/151/0>. (Visited on June 10, 2025).

<sup>7</sup> Ministry of Corporate Affairs, *Notification* S.O. 3199(E) (July 18, 2023), available at: <https://www.cci.gov.in/legal-framework/notifications/details/158/0>. (Visited on June 10, 2025)

<sup>8</sup> Ministry of Corporate Affairs, *Notification* S.O. 4672(E) (October 26, 2023), available at: <https://www.cci.gov.in/legal-framework/notifications/details/159/0>. (Visited on June 10, 2025).

<sup>9</sup> Ministry of Corporate Affairs, *Notification* S.O. 740(E) (February 19, 2024), available at: <https://www.cci.gov.in/legal-framework/notifications/details/160/0>. (Visited on June 10, 2025).

<sup>10</sup> Ministry of Corporate Affairs, *Notification* S.O. 1065(E) (March 05, 2024), available at: <https://www.cci.gov.in/legal-framework/notifications/details/161/0>. (Visited on June 10, 2025).

<sup>11</sup> Ministry of Corporate Affairs, *Notification* S.O. 3846(E) (September 9, 2024), available at: <https://www.cci.gov.in/legal-framework/notifications/details/162/0>. (Visited on June 10, 2025).

<sup>12</sup> Ministry of Corporate Affairs, *Notification* S.O. 4031(E) (September 19, 2024), available at: <https://www.cci.gov.in/legal-framework/notifications/details/163/0>. (Visited on June 10, 2025).

This proviso specifically recognizes the ‘hub and spoke cartel’. Before the amendment, in *Samir Agrawal v. ANI Technologies Pvt. Ltd.*,<sup>13</sup> a case where it is alleged that the pricing mechanism adopted by Ola and Uber, which takes away the liberty of drivers to compete with each other, violates section 3, the CCI, while finding that there is no hub-and-spoke cartel, held that,<sup>14</sup> “For a cartel to operate as a hub and spoke, there needs to be a conspiracy to fix prices, which requires the existence of collusion in the first place. In the present case, the drivers may have acceded to the algorithmically determined prices by the platform, this cannot be said to be amounting to collusion between the drivers. In the case of ride-sourcing and ride-sharing services, a hub-and-spoke cartel would require an agreement between all drivers to set prices through the platform, or an agreement for the platform to coordinate prices between them. There does not appear to be any such agreement between drivers inter-se to delegate this pricing power to the platform/cab aggregators.”

In this case, the CCI reflected that there had to be an active collusion to establish a hub and spoke cartel. However, by the 2023 amendment, the CCI can scrutinize a hub even if it does not actually participate in facilitating a cartel as long as the CCI can show that the hub intended to participate.

#### Tie-in arrangement

The definition of tie-in arrangement under section 3(4) has been amended to expressly provide that the tied and tying products must be distinct or separate goods and services. This is in tune with the decisional practice of the CCI.

#### Exclusive Dealing Agreement

The term ‘exclusive supply agreement’ has been replaced by the term ‘exclusive dealing agreement’ under section 3(4) to expressly recognize the exclusivity imposed from the sellers’ and buyers’ sides.

#### General IPR Defence Clause

Under section 3(5), clause (g) has been added to provide, “any other law for the time being in force relating to the protection of other intellectual property rights.” Specific exceptions exist for particular IPRs: copyright, patents, trademarks, geographical indications, designs, and layout-design of semiconductor integrated circuits.

---

<sup>13</sup> 2018 SCC OnLine CCI 86.

<sup>14</sup> *Id.* para. 15.

## Regulation of Combinations

### Timelines for filing and review of combinations

The timelines for filing and review of the combinations by the CCI were amended in the following manner:

	Pre-amendment	Post-amendment
The enterprise shall give notice to the CCI of the proposed combination (Section 6(2))	Within 30 days of approval of the proposal by the board of directors or execution of any agreement or other document	The 30-day time period was deleted, and now the enterprise shall give notice to the CCI of the proposed combination after the approval of the proposal by the board of directors or execution of any agreement or other document, but before the consummation of the combination.
Overall timeline for review of combination (Section 6(2A))	210 days from the notice given to the CCI under section 6(2) or the CCI has passed orders under section 31, whichever is earlier.	150 days have passed since the day the notice was given to the CCI under section 6(2), or the CCI has passed orders under section 31, whichever is earlier.
CCI forms a prima facie opinion that the combination is likely to cause or has caused AAEC (Section 29(1)).	No time period for forming a prima facie opinion.	Section 29(1B) was inserted- CCI shall form its prima facie opinion within 30 days of receipt of notice.  Proviso to Section 31(1) was inserted- If CCI does not form a prima facie opinion under Section 29(1B), the combination shall be deemed approved, and no separate order shall be required.

Parties to respond to the show cause notice issued by CCI (Section 29(1)).	Within 30 days of the receipt of the notice.	Within 15 days of the receipt of the notice.
CCI again forms a prima facie opinion and directs parties to publish details of the combination (Section 29(2)).	Within seven working days from receipt of the parties' response to the combination.	Within seven days from receipt of the parties' response to the combination.
Parties are to publish details of the combination on the direction of the CCI (Section 29(2)).	Within 10 working days of such direction.	Within seven days of such direction.
CCI may invite the public or anyone to file written objections (Section 29(3)).	Such objections can be filed within 15 working days from the date on which details of the combination were published.	Such objections can be filed within 10 days from the date on which details of the combination were published.
CCI may call for additional information from parties (Section 29(4)).	Within 15 working days from the expiry of the period specified in section 29(3).	Within 7 days from the expiry of the period specified in section 29(3).
Parties to file additional information (Section 29(5)).	Within 15 working days from the expiry of the period specified in section 29(4).	Within 10 days from the expiry of the period specified in section 29(4).
After receipt of all information	CCI shall proceed to deal with the case as per section 31 within 45 working days from the expiry of the period specified in section 29(5).	CCI shall deal with the case as per section 29A or section 31.
<p>Insertion of Section 29A- It provides:</p> <ul style="list-style-type: none"> <li>CCI will issue a statement of objections to the parties identifying AAEC.</li> </ul>		

- CCI will direct parties to explain within 25 days of receipt of the statement of objections why such a combination should be allowed to take effect.
- The parties may submit an offer of appropriate modification.
- If CCI does not accept the modification, it shall communicate to the parties why the modification is insufficient to eliminate the AAEC within 7 days from receipt of the proposed modification.
- CCI shall call upon the parties to submit a revised modification within 12 days of receiving such communication.
- CCI shall evaluate such revised proposal for modification within 12 days from receipt of such proposal.
- CCI may suo moto propose appropriate modifications.

The timelines in the newly inserted section 29A were not there before the amendment.

### Deal Value Threshold

The combinations under section 5 were assessed based on assets or turnover thresholds. However, with the expansion of digital markets, it was realized that enterprises in digital markets usually fail to generate revenue for several years and are traditionally asset-light. Therefore, it was essential to introduce a deal value threshold so that the CCI could also assess high-value transactions in digital markets.<sup>15</sup>

The amendment under section 5 inserted the deal value threshold. If the value of any transaction exceeds 2000 crore, then such a transaction related to the acquisition of any control, shares, voting rights, or assets of an enterprise, merger, or amalgamation needs to be notified to the CCI. Provided that the enterprise that is being acquired, taken control of, merged, or amalgamated should have substantial business operations in India. The inclusive definition of the term 'value of transaction' was inserted by the amendment in Explanation (d) to section 5. It includes "every valuable consideration, whether direct or indirect, or deferred for any acquisition, merger, or amalgamation." Regulation 4 of the CCI (Combinations) Regulations, 2024, has clarified what is included in the terms 'value of transaction' and 'substantial business operations in India'.

### De Minimis Exemption

---

<sup>15</sup> *Supra* note 3 at 158.

Before the amendment, the Central Government, by notifications dated March 27, 2017, while exercising its powers under section 54(a), exempted certain combinations based on assets and turnover from the provisions of section 5 for 5 years. After the amendment, the de minimis exemption was inserted under section 5. It provides, "...where either the value of assets or turnover of the enterprise being acquired, taken control of, merged or amalgamated in India is not more than such value as may be prescribed, such acquisition, control, merger or amalgamation, shall not constitute a combination under section 5." The de minimis exemption does not apply to the deal value threshold.

After the amendment, the Central Government, by notification dated March 7, 2024, while exercising its powers under section 54(a), exempted a specific combination from the provisions of section 5 for 2 years. The Central Government has notified the Competition (Minimum Value of Assets or Turnover) Rules, 2024 on September 9, 2024, whereby it provides the value of assets and turnover for de minimis exemption under section 5.

The thresholds for the de minimis exemption through various notifications are as follows:

	Notification dated March 27, 2017	Notification dated March 7, 2024	Competition (Minimum Value of Assets or Turnover) Rules, 2024
Assets	Not more than 350 crores	Not more than 450 crores	Not more than 450 crores
Turnover	Not more than 1000 crores	Not more than 1250 crores	Not more than 1250 crores

#### Definition of 'Control'

Before the amendment, the definition of control under section 5 was inclusive. It included, "controlling the affairs or management..." There was no clarity on what rights may amount to control, which caused the CCI to give different interpretations. In some cases, the CCI has used the test of ability to exercise 'decisive influence'<sup>16</sup> and in others' ability to exercise 'material influence'.<sup>17</sup>

<sup>16</sup> CCI, *Independent Media Trust/RB Mediasoft Pvt. Ltd.*: Combination Registration No. C-2012/03/47 dated May 28, 2012.

<sup>17</sup> CCI, *UltraTech Cement Limited/Jaiprakash Associates Limited*: Combination Registration No. C-2015/02/246 dated March 12, 2018; CCI, *Agrium Inc./Potash Corporation of Saskatchewan Inc.*: Combination Registration No. C-2016/10/443 dated October 27, 2017.

The definition of the term ‘control’ under section 5 has been amended, and much-needed clarity has been brought forth in the definition. Post amendment means the “ability to exercise material influence over the management or affairs or strategic commercial decision.” However, the Amendment Act does not define ‘material influence’. The CCI in one of its orders,<sup>18</sup> defined ‘material influence’ as, “...the lowest level of control, implies presence of factors which give an enterprise the ability to influence affairs and management of the other enterprise, including factors such as shareholding, special rights, status and expertise of an enterprise or person, board representation, structural/financial arrangements, etc.” The CLRC, in its report, had proposed that it is essential to have clear guidelines as to what constitutes ‘material influence’ through subordinate legislation.<sup>19</sup> Yet, the CCI does not have such guidelines.

#### Definition of ‘Group’

The definition of the term ‘group’ was amended. It means “two or more enterprises where one enterprise is directly or indirectly, in a position to- (i) exercise twenty-six percent or such other higher percentage as may be prescribed, of the voting rights in the other enterprise....” Before the amendment the group was defined to mean “two or more enterprises which, directly or indirectly, are in a position to....” The definition was interpreted to mean that a group can only comprise of three or more enterprises where two or more enterprises exercised some control over the other. This would lead to the interpretation that a holding company and a subsidiary company can never be a group. To avoid this anomaly, the words were substituted with “two or more enterprises where one enterprise is directly or indirectly, in a position to...”

Also, before the amendment, the Central Government exempted the group for 5 years, exercising less than fifty percent of voting rights in other enterprises from the provisions of section 5 by exercising the powers under section 54(a).<sup>20</sup> The amendment by adding the words “...such other higher percentage as may be prescribed, of the voting rights in the other enterprise ...” provides flexibility, and the threshold may be amended as required, looking at the evolution of the market.

#### Computation of ‘Turnover’

The act contained an inclusive definition of ‘turnover’ under section 2(y). It includes “value of sale of goods or services.” The definition is broad and does not indicate the manner of computing turnover specifically to assess a combination based on the turnover threshold. In its frequently

---

<sup>18</sup> CCI, *UltraTech Cement Limited/Jaiprakash Associates Limited*: Combination Registration No. C-2015/02/246 dated March 12, 2018

<sup>19</sup> *Supra* note 3 at 120.

<sup>20</sup> Ministry of Corporate Affairs, Notification dated March 4, 2016, available at: [https://www.cci.gov.in/uploads/filemanager/catalog/faqs/SO%20673\(E\)-674\(E\)-675\(E\).pdf](https://www.cci.gov.in/uploads/filemanager/catalog/faqs/SO%20673(E)-674(E)-675(E).pdf). (Visited on May 30, 2025).

asked questions (FAQs), the CCI excluded indirect taxes, income from ancillary operations, and intra-group sales from the turnover. However, the FAQs are not considered binding instruments; they are only for guidance. To clarify this, the methodology of computation of turnover was inserted in the Explanation(c) to section 5.

It means:

“the turnover certified by the statutory auditor on the basis of the last available audited accounts of the company in the financial year immediately preceding the financial year in which the notice is filed under sub-section (2) or sub-section (4) of section 6 and such turnover in India shall be determined by excluding intra-group sales, indirect taxes, trade discounts and all amounts generated through assets or business from customers outside India, as certified by the statutory auditor on the basis of the last available audited accounts of the company in the financial year immediately preceding the financial year in which the notice is filed under sub-section (2) or sub-section (4) of section 6.”

It includes the turnover certified by the statutory auditor and excludes intra-group sales, indirect taxes, trade discounts, and all amounts generated through assets or business from customers outside India.

Green Channel

The amendment has incorporated the green channel into the Act. Before the amendment, in August 2019, the CCI introduced a green channel for automatic approval of combinations through regulations. The amended section 6(4) provides that if a combination fulfils the prescribed criteria, then notice of such combination may be given as specified in regulations. No separate notice is required under 6(2). As per section 6(5), the proposed combination shall be deemed approved by the CCI upon filing a notice and acknowledgment. Further, according to section 6(6), if within one year from the date on which such combination has taken effect, the CCI finds that the combination does not fulfil the requirements or materially incorrect or incomplete declarations have been filed, the approval shall be void ab initio and the CCI may pass order as it may deem fit. However, no such order shall be passed without giving the parties to the combination an opportunity to be heard.

The Central Government has notified the Competition (Criteria of Combination) Rules, 2024 on September 9, 2024. These rules prescribe which combinations can go through the green channel route. Rule 3 provides that the parties to the combination, their respective group entities<sup>21</sup> and

---

<sup>21</sup> Rule 3(2)(a) of the Competition (Criteria of Combination) Rules, 2024 provides that, “the parties to the combination and their respective group entities means- (i) the ultimate controlling person of the acquirer and other

their affiliates<sup>22</sup> “should not produce or provide similar or identical or substitutable product or service; should not be engaged in any activity relating to production, supply, distribution, storage, sale and service or trade in product or provision of service which are at different stage or level of production or which are complementary to each other.” The green channel route is available to parties without horizontal, vertical, or complementary overlap.

### Open Market Transactions

In India, before the amendment, no part of the combination could be consummated without the prior approval of the CCI as per sections 6(2A) and 43. The amendment allows open market transactions by the newly inserted section 6A. It provides that:

“Nothing contained in sub-section (2A) of section 6 and section 43A shall prevent the implementation of an open offer or an acquisition of shares or securities convertible into other securities from various sellers, through a series of transactions on a regulated stock exchange, from coming into effect, if—

(a) the notice of the acquisition is filed with the Commission within such time and in such manner as may be specified by regulations; and

(b) the acquirer does not exercise any ownership or beneficial rights or interest in such shares or convertible securities including voting rights and receipt of dividends or any other distributions, except as may be specified by regulations, till the Commission approves such acquisition in accordance with the provisions of sub-section (2A) of section 6 of the Act.”

### Procedural Changes

The procedure for inquiry under section 26 has been reviewed to include the following:

- Section 26(2A) has been inserted to enable the CCI not to inquire if the same or substantially the same facts and issues were raised in any information received under section 19 or in any reference from the Central Government or a State Government or statutory authority, and the CCI has already decided the same in its previous order. This provision is to avoid multiplicity of proceedings before the CCI.

---

entities forming part of the same group; (ii) the enterprise being acquired and its downstream entities forming part of its group; (iii) enterprises being merged or amalgamated, their controlling persons, and entities forming part of their group.”

<sup>22</sup> Rule 3(2)(b) of the Competition (Criteria of Combination) Rules, 2024 provides that, “an enterprise is considered to be an affiliate of another enterprise if that other enterprise has- (i) ten per cent or more of the shareholding or voting rights of the enterprise; or (ii) right or ability to have a representation on the board of directors of the enterprise either as a director or as an observer; or (iii) right or ability to access commercially sensitive information of the enterprise.”

- Sections 26(3A) and 26(3B) have been inserted to empower the CCI to direct the Director-General (DG) to investigate the matter further and to submit a supplementary report.
- Section 26(9) has been added to enable the CCI to pass orders for closure of cases on completion of the investigation or inquiry.

## **Global Turnover**

Section 27(b) of the Act empowers the CCI to impose a penalty for violating sections 3 or 4. The penalty shall not exceed ten per cent of the average turnover or income for the last three financial years. However, in case of a cartel, a penalty of up to three times the profit or ten percent of the turnover, whichever is higher, can be imposed.

The Amendment Act has inserted two explanations. Explanation 1 provides that turnover shall be determined as regulations may provide. Explanation 2 states, “turnover means global turnover derived from all the products and services by a person or an enterprise.”

Before the Amendment Act, the interpretation of the term turnover under section 27 was at issue before the Supreme Court in the case of *Excel Crop Care v. Competition Commission of India*.<sup>23</sup> Relying upon the doctrine of proportionality<sup>24</sup> and purposive interpretation<sup>25</sup>, the Supreme Court held that the penalty under section 27(b) shall be determined based on relevant turnover as opposed to the total turnover. The court observed that:<sup>26</sup>

“In the absence of specific provision as to whether such turnover has to be product specific or entire turnover of the offending company, we find that adopting the criteria of relevant turnover for the purpose of imposition of penalty will be more in tune with the ethos of the Act....”

The court further observed that:<sup>27</sup>

“When the agreement leading to contravention of section 3 involves one product, there seems to be no justification for including other products of an enterprise for the purpose of imposing penalty. This is also clear from the opening words of section 27 read with

---

<sup>23</sup> (2017) 8 SCC 47.

<sup>24</sup> *Id.* para. 92.

<sup>25</sup> *Id.* para. 94.

<sup>26</sup> *Id.* para. 83.

<sup>27</sup> *Id.* para. 91.

section 3 which relate to one or more specified products. It also defies common sense that though penalty would be imposed in respect of the infringing product, the maximum penalty imposed in all cases be prescribed on the basis of all the products and the total turnover of the enterprise, it would be more so when total turnover of an enterprise may involve activities besides production and sale of products, like rendering of services, etc. It, therefore, leads to the conclusion that the turnover has to be of the infringing products and when that is the proper yardstick, it brings home the concept of relevant turnover.”

It is clear from the observation in this case, that the Supreme Court decided in favour of relevant turnover as opposed to total turnover. After this judgment, the CCI imposed a penalty based on relevant turnover; however, it expressed its concerns about applying the concept of relevant turnover to digital market platforms. In *Federation of Hotel & Restaurant Associations of India v. MakeMyTrip India Pvt. Ltd.*,<sup>28</sup> the CCI imposed a penalty on the entire turnover of MMT-Go and OYO for violation of sections 3 and 4. The CCI held that:<sup>29</sup>

“In case of digital market platforms, restricting revenue to just one segment would not appropriately capture the interdependent and integrated nature of the ecosystem wherein one product/service reinforces multiple other products/services. This approach might be appropriate in traditional markets, but not so much so in case of two-sided or multi-sided platforms. In such platforms, not only two user sides are interacting and thus, intricately intertwined with each other, but the products/services offered by the platform operator through other verticals also derive strength from each other due to economies of scope and scale. Accordingly, in such markets, for the purposes of revenue determination, the entire platform has to be taken as one unit. Any other interpretation or approach would render the deterrence exerted by the statute as redundant and nugatory.”

Similarly, in *Matrimony.com Limited v. Google*,<sup>30</sup> the CCI found Google violating section 4 of the act and imposed a penalty on their total revenue generated from India operations from different business segments rather than any specified services. Though the CCI considered the revenue generated from India only and not the revenue generated by Google globally, it recorded its concern regarding the relevant turnover:<sup>31</sup>

“...the concept of relevant turnover cannot be applied to a technological platform such as google as it is applied in the context of a conventional multi-product company. In a two sided

---

<sup>28</sup> CCI, Case No. 14 of 2019, Order dated 19.10.2022.

<sup>29</sup> *Id.* para. 319.

<sup>30</sup> CCI, Case No. 07 and 30 of 2012, Order dated 08.02.2018.

<sup>31</sup> *Id.* para. 431.

market, the search side is free whereas the other side is monetized through advertisements. It would stultify the very object and intendment of the Act if Google were to be allowed to contend that search being free, no penalty can be levied as there is no revenue stream from this side of the market. Such a pedantic approach, which is more appropriate for conventional market, would virtually allow two sided platforms to abuse one side and accord a virtual immunity from monetary penalty for anti-trust violations...the entire platform has to be taken as one unit and revenue generated therefrom has to be seen as a whole. Any other interpretation or approach would render the deterrence exerted by the statute as redundant and nugatory.”

The CCI followed a similar approach in XYZ v. Google<sup>32</sup> and Umar Javeed v. Google<sup>33</sup> while imposing a penalty on Google for violating section 4 of the act. The CCI also faced the problem regarding the imposition of a penalty on relevant turnover in the case of cover bidding in Nagrik Chetna Manch v. Fortified Security Solutions,<sup>34</sup> where a few opposite parties were not engaged in manufacturing the relevant product. The CCI still imposed the penalty on the total turnover of such opposite parties and held that,<sup>35</sup> “...imposition of penalty on the basis of relevant turnover in this case would imply that no penalty would be leviable on several opposite parties who have indulged in bid-rigging in contravention of the provisions of the Act. This would result in an anomalous situation and would render the objective of the Act infructuous.”

These cases reflect that the CCI was facing issues in imposing a penalty on relevant turnover, specifically in the case of violations by digital market platforms or technological platforms. The concern was also discussed in the CLRC Report, which specifically highlighted that if the concept of relevant turnover is followed, then it will be difficult for the CCI to impose any penalty on hubs in case of a hub and spoke cartel, as the hub is not engaged in the same business as that of the spokes.<sup>36</sup> Accordingly, the CLRC Report recommended that the term turnover should not be replaced by the term ‘relevant turnover’ in section 27(b); instead, the concept of

---

<sup>32</sup> CCI, Case No. 7 of 2020, Order dated 25.10.2022, para. 407. The CCI held that, “...to determine relevant turnover in relation to technology platforms, such as one operated by Google, it is important to appreciate the business model, incentives of the platforms and their revenue streams. Various products of Google work on the basis of network effects i.e., with the increase in number of users on its platform, the attractiveness of the platform/products for the advertisers increases multi-fold. In such platforms, not only two/multi sides are intricately intertwined and interwoven with each other, but the products/services offered by the platform operator derive strength from each other due to economies of scope and scale. Replicating such an ecosystem becomes extremely difficult for a new entrant. Competition in such a scenario is amongst ecosystems and not just the verticals or independent services. In such a case, the entire platform has to be taken as one unit to account for the cross-market externalities between platform sides, and revenue generated therefrom has to be seen as a whole.”

<sup>33</sup> CCI, Case No. 39 of 2018, Order dated 20.10.2022.

<sup>34</sup> CCI, Case No. 50 of 2015, Order dated 01.05.2018.

<sup>35</sup> *Id.* para. 96.

<sup>36</sup> *Supra* note 3 at 79, 80.

‘relevant turnover’ should be introduced by the guidelines/regulations. Accordingly, the report recommended that the CCI issue guidance on imposing penalties.

The Draft Amendment Bill, 2020, proposed the insertion of a proviso in section 27(b), which specifically provided that, “the turnover...shall be determined in such manner as may be prescribed.” This was also followed in the Amendment Bill, 2022, which, on similar lines, proposed to introduce an explanation to section 27(b). Accordingly, Explanation 1 was introduced by the Amendment Act, 2023, which mandates the CCI to formulate regulations for determining turnover to impose a penalty. This amendment has considered the concerns of the CCI in the cases discussed above.

It is pertinent to mention that the Explanation 2 introduced in section 27(b) for imposing a penalty on global turnover was not proposed in the Draft Amendment Bill, 2020, nor in the Amendment Bill, 2022. Similarly, the same was not recommended in the CLRC or SCF reports. Therefore, this amendment has been criticized because no feedback was ever taken from the stakeholders, and the same was not even discussed in any of the reports. Also, some have argued that this amendment overturns the decision of the Supreme Court in *Excel Crop Care*<sup>37</sup> case as it permits the CCI to impose a penalty on the global turnover from all the products and services, which will significantly impact companies with a multi-product profile and international presence, in contrast to companies with domestic presence.

A collective reading of both the explanations as introduced by the Amendment Act, 2023, leaves a scope for the CCI to formulate penalty regulations after taking into consideration the judgment of the Supreme Court in the *Excel Crop Care* case and the issues that the CCI faced while imposing a penalty based on relevant turnover in the cases discussed above.

The CCI has notified the CCI (Determination of Turnover or Income) Regulations, 2024 on March 6, 2024. Regulation 3 provides:

- Inclusion: Turnover includes the total value of sales or revenue or receipts and other operating income.
- Exclusion: Turnover excludes indirect taxes, trade discounts, and intra-group sales.
- Determination: Turnover shall be determined based on audited consolidated financial statements, and in case it is not available, turnover will be the amount certified by the statutory auditor of the enterprise, and if such statutory auditor is not appointed, then it will be the amount certified by the Chartered Accountant.

---

<sup>37</sup> *Supra* note 23.

The CCI has also notified the CCI (Determination of Monetary Penalty) Guidelines, 2024 on March 6, 2024. Guideline 2(h) defines the term ‘relevant turnover’. It means “the turnover derived by an enterprise directly or indirectly from the sale of products and/or provision of services, to which the contravention relates and determined for imposition of penalty.” According to Guideline 3(1), the CCI would consider an amount up to thirty percent of the relevant turnover, having regard to the following factors:

- Nature and gravity of the contravention,
- Nature of the industry or sector affected by the contravention and its implications on the economy,
- Any other factor.

According to Guideline 3(2), the CCI may impose a penalty by adjusting the amount so determined after considering the following factors:

- Duration of the contravention.
- Role of the enterprise in the contravention.
- Whether any coercive or retaliatory measures were taken against other enterprises to participate in the contravention.
- Repeated contravention.
- When the enterprise admits to contravention and the stage at which such admission is made.
- The evidence furnished by the enterprise that establishes its limited involvement in the contravention.
- Extent of cooperation by the enterprise during the DG’s investigation and proceedings before the CCI.
- Voluntary termination of alleged conduct under intimation to the CCI.
- Implementation of a Competition Compliance Programme within the enterprise.
- Any other factor.

According to Guideline 3(3), the CCI may consider the relevant turnover of three years of the enterprise preceding the year the CCI receives the DG’s investigation report. However, in some cases, for the reasons to be recorded in writing, the CCI may consider the relevant turnover of three years preceding the contravention. According to Guideline 3(6), if it is not feasible to determine relevant turnover, then the CCI may consider the global turnover, derived from all products and services, for determining the penalty. These guidelines have brought forth the clarity required and are in tune with the judgment of the Supreme Court in the Excel Crop Care case.

## **Commitment and Settlement**

The Amendment Act has introduced a legal framework for ‘Commitment and Settlement’ under sections 48A and 48B. Before the amendment, no specific provisions dealing with commitment or settlement existed.

Before the amendment, in *The Tamil Nadu Film Exhibitors Association v. CCI*,<sup>38</sup> the Madras High Court held that:<sup>39</sup>

“...we do not see any reason as to why the Scheme of the Competition Act, 2002 should be taken to prohibit any settlement, especially when the scope of Section 27 of the Act is very wide, conferring jurisdiction upon the Commission to pass residuary orders...it is possible within the framework and scheme of the Competition Act, 2002 to allow settlements and compromises to be reached between parties, provided the Commission is of considered view that such settlements and compromises would not lead to the continuance of anti-competitive practice, would not allow the abuse of dominant position to continue and would not be prejudicial to the interest of consumers or to the freedom of trade.”

This observation made it abundantly clear that settlement was within the scope of the act; however, there was no specific provision for the same, and the CCI had to rely upon the residuary clause under section 27(g).

The provisions for settlement and commitment are available only for the violation of sections 3(4) and 4, not for the violation of section 3(3), which includes cartels and horizontal agreements. Before the amendment, suggestions were furnished to widen the settlement and commitment provisions to include offences under section 3(3).<sup>40</sup> However, these suggestions were not accepted because of the leniency provisions available for violating section 3(3). Also, cartels and horizontal agreements under section 3(3) are pernicious; therefore, keeping them out of the settlement and commitment framework was considered appropriate.<sup>41</sup>

Section 48A deals with settlement. It provides that if any inquiry has been initiated against an enterprise for contravention of section 3(4) or section 4, it may submit an application for settlement of the proceeding to the CCI. Such an application must be submitted after receipt of the Director General's report under section 26(4) but before the CCI passes any order under

---

<sup>38</sup> (2015) 2 LW 686 (DB).

<sup>39</sup> *Id.* at 696.

<sup>40</sup> *Supra* note 5.

<sup>41</sup> *Id.* at 33-34.

section 27 or section 28. After considering the nature, gravity, and impact of the contraventions, the CCI may accept the proposal for settlement on payment of an amount or on such terms as may be specified by regulations. The CCI can reject the settlement application if it thinks the settlement offered is inappropriate. In case of rejection, the CCI can proceed with the inquiry under section 26.

Section 48B deals with commitment. It provides that if any inquiry has been initiated against an enterprise for contravention of section 3(4) or section 4, it may submit an application offering commitments. It can be submitted at any time after an order under section 26(1) has been passed but before the receipt of the report of the Director General under section 26(4). After considering the nature, gravity, and impact of the contraventions, the CCI may accept the proposed commitments. The CCI can reject the commitment offered if it thinks that the commitment offered is not appropriate. In case of rejection, the CCI can proceed with the inquiry under section 26.

No appeal is available under section 53B against the order passed by the CCI under sections 48A and 48B. However, such an order may be revoked under section 48C if an applicant fails to comply with the order, or the applicant has not made full and true disclosure, or there has been a material change in the facts. Further, such an enterprise shall be liable to pay legal costs, which may extend to one crore rupees. After revocation, the CCI may restore or initiate the inquiry.

The CCI has also notified the CCI (Settlement) Regulations, 2024, and the CCI (Commitment) Regulations, 2024, on March 6, 2024, laying down the procedure for settlement and commitment applications.

### **Leniency Plus Regime**

The Amendment Act has brought two significant changes to the existing leniency regime. Firstly, the CCI can permit an applicant to withdraw its application for lesser penalty and secondly, when an applicant who has disclosed a cartel also discloses another cartel, which enables CCI to form prima facie opinion that there exists another cartel, in such a case, the CCI may impose lesser penalty in respect of the cartel under investigation without prejudice to the applicant obtaining lesser penalty regarding the newly disclosed cartel.

## **Other Changes**

- **Definition of Relevant Product Market (RPM):** In the parent act, under section 2(t), the RPM was understood only from the consumer side or demand side substitutability; however, by the amendment in the year 2023, now the definition incorporates both demand side substitutability as well as supply side substitutability. It incorporates explicitly that RPM means a market comprising of all the products or services which are, “...considered interchangeable or substitutable by the supplier, by reason of the ease of switching production between such products and services and marketing them in the short term without incurring significant additional costs or risks in response to small and permanent changes in relative prices.” This amendment has made the definition more comprehensive. It gives discretion to the CCI to delineate RPM based on demand side substitutability, supply side substitutability, or both, based on the facts of the case. Even before the amendment, the CCI in a few instances had delineated RPM based on supply-side substitutability.<sup>42</sup>
- **Additional restriction on the employment of members of the CCI:** Under section 12 of the parent act, the chairperson and members of the CCI are not allowed to accept any employment in any enterprise that was a party before the CCI for two years from the date on which they cease to hold office. This provision only bars the employment; therefore, the chairperson and members of the CCI could have acted in an advisory capacity. To overcome this, the 2023 amendment bars the chairperson and members from advising as a consultant, retainer, or in any capacity for such enterprises. After the 2023 amendment, under section 12, additional restrictions have been imposed apart from the existing restrictions under the parent act. The chairperson and members of the CCI post-retirement are not allowed to represent any person or enterprise before the CCI. Also, they are not allowed to accept any employment or give any advice to any person who appears before the CCI under section 35.
- **Introduction of limitation period:** The 2023 amendment has introduced a limitation period of three years from the date of the cause of action to entertain any information or reference by the CCI under section 19 of the act. However, if there is sufficient cause for

---

<sup>42</sup> See, CCI, *Department of Sports v. Athletics Federation of India*, Ref Case No. 01 of 2015, Order dated 12.07.2018. In this case, the CCI delineated RPM on the basis of both demand and supply side substitutability and decided it to be “provision of services relating to organization of athletics/athletic activities in India”.

not filing it within such period, the CCI is empowered to condone the delay after recording its reasons.

- **No casting vote for the Chairperson of the CCI:** By the 2023 amendment, under section 22(3), the provision regarding the second or casting vote of the Chairperson in the case of equality of votes has been deleted. This aligns with the judgment of the Delhi High Court in *Mahindra Electric Mobility Limited v. CCI*.<sup>43</sup> In this case, the court held that the casting vote given to the Chairperson under section 22(3) is unconstitutional. The court observed that, "... there can be no two opinions that a casting vote, which potentially can lead to as adjudicatory result or consequence, is anathema to and destroys the Rule of Law in the context of Indian Constitution."<sup>44</sup>
- **Appointment of Director General (DG):** Before the 2023 amendment, the appointment of DG was with the Central Government under section 16 of the parent act. However, after the amendment, the appointment of the DG is with the CCI; however, the approval of the Central Government is required for the same.
- **Powers of DG:** Section 41 of the parent act has been amended by the 2023 Amendment Act to give more powers to DG. The DG is empowered to keep in his custody any information or documents necessary for investigation for 180 days, and after that, the DG is bound to return the same. However, if such information or documents are required again, the DG may call the same by a written order for an additional period of 180 days. If during the investigation, the DG has reasonable grounds to believe that any information or any documents may be destroyed, the DG can make an application to the Chief Metropolitan Magistrate (CMM), Delhi, for an order of seizure. The DG is further empowered to examine any of the employees of the party being investigated and any other person, but only with the approval of the CCI. Such examination has to be recorded in writing and signed by the person examined and may be used as evidence. The DG is permitted to requisition the services of police or any officer of the Central Government for assistance. The CMM, Delhi, may, based on an application and after hearing the DG, authorize the DG to enter any place where any information or documents are kept, search that place, and seize such information or documents.

---

<sup>43</sup> 2019 SCC OnLine Del 8032.

<sup>44</sup> *Id.* para. 160.

- **Enhanced penalty:** Section 44 has been amended to enhance the penalty from 1 crore to 5 crore for making a false statement or omission to furnish material information.
- **Pre-Deposit of penalty for appeal:** Section 53B has been amended to mandate deposit of 25% of the penalty amount for filing an appeal before the Appellate Tribunal.
- **Enabling parties to call experts:** Section 35 has been amended by the insertion of sub-section (2), enabling parties to call experts in any field to provide an expert opinion in connection with any matter.
- **Transparency in issuing regulations:** Section 64A mandates CCI to ensure transparency while making regulations. The CCI shall publish draft regulations and invite public comments; publish a statement of its response to the public comments, and periodically review such regulations.
- **CCI to issue guidelines:** The newly inserted section 64B empowers CCI to publish guidelines suo moto or on a request. It is clarified in the section itself that such guidelines shall not be construed as a determination of any question of fact or law by the CCI and shall not be binding.
- **Decriminalization of certain offences:** Certain provisions like sections 42, 43, and 45 were amended, and the words ‘punishable with fine’ have been substituted with ‘liable for penalty’, and specifically in section 45, the word ‘offences’ is substituted with ‘contraventions’.
- **Compounding of certain offences by NCLAT:** The newly inserted section 59A provides that any offence punishable under this Act not being an offence punishable with imprisonment only or imprisonment and also with fine may be compounded by the NCLAT either before or after the institution of any proceeding.

### **III. Conclusion**

The Competition Amendment Act, 2023, has incorporated considerable changes in the Competition Act, 2002, which aimed at strengthening competition regulation and fostering a business-friendly environment. The multiple changes in the procedural timelines for approving combinations will provide certainty and will facilitate faster approvals of transactions. The introduction of the settlement and commitment framework will help in the faster resolution of

complaints and will reduce litigation. These amendments will improve the ease of doing business. The introduction of the deal value threshold will ensure that the high-value deals, specifically in the digital markets, are reviewed by the CCI, which will address the big data and privacy issues. Introduction of a limitation period for filing cases, penalties linked to global turnover, and the guidelines issued on it, amendments to certain definitions like control, group, turnover, and relevant product market, and explicit recognition of hub and spoke cartel will strengthen the enforcement mechanism and bring predictability.

However, the following issues were not addressed in the Amendment Act, 2023:

- **Collective Dominance:** The Competition (Amendment) Bill, 2012, proposed the specific recognition of the concept of ‘collective dominance’ by amending section 4(1) by inserting the terms ‘jointly or singly’ directly after the words ‘or group’. In many instances before the CCI,<sup>45</sup> the issue of collective dominance was raised, and the CCI maintained that the Act does not recognize the concept of collective dominance. The legislature missed the opportunity to specifically recognize collective dominance by the Amendment Act, 2023, as done by many countries.
- **Buyers’ Cartel:** The Draft Competition (Amendment) Bill, 2020, specifically recognized the buyers’ cartel by amending the definition of cartel in section 2(c). However, it is not addressed in the Amendment Act, 2023. The CCI initially refused to recognize the concept of buyers’ cartel;<sup>46</sup> however, with time, the CCI has recognized that section 3(3) covers both sellers’ and buyers’ cartels.<sup>47</sup> Therefore, it was desirable to explicitly recognize a buyers’ cartel under the Act.
- **Judicial member in CCI:** In *Mahindra Electric Mobility Limited v. CCI*,<sup>48</sup> the High Court of Delhi observed that, “...when adjudicatory orders (especially final orders) are made by CCI, the presence and participation of the judicial member is necessary.” The CLRC, in its report, left it to the Central Government to consider necessary action for the implementation of the judgment.<sup>49</sup> However, some of the members of the CLRC, like Mrs. Pallavi Shroff<sup>50</sup> and Dr. S Chakravarthy<sup>51</sup>, expressed certain reservations and pointed out that every panel of the CCI must have a judicial member.

---

<sup>45</sup> See, *Dish TV India v. Hathway Cable*, [2014] CCI 55, *Meru Travel Solutions (P) Ltd. v. ANI Technologies (P) Ltd.*, 2018 SCC OnLine CCI 46, *Ashok Kumar Vallabhaneni v. Geetha SP Entertainment LLP*, 2019 SCC OnLine CCI 27 and *Samir Agrawal v. CCI*, (2021) 3SCC 136.

<sup>46</sup> *Pandrol Rahee Technologies Pvt. Ltd. v. Delhi Metro Rail Corporation*, 2011 SCC OnLine CCI 64.

<sup>47</sup> *XYZ v. Indian Oil Corporation Ltd.*, 2018 SCC OnLine CCI 55, and *Gujarat Paper Mills Association v. Indian Corrugated Case Manufacturers’ Association*, 2021 SCC OnLine CCI 13.

<sup>48</sup> *Supra* note 43.

<sup>49</sup> *Supra* note 3 at 37.

<sup>50</sup> *Id.* at 197-198.

<sup>51</sup> *Id.* at 212.

The SCF, in its report, noted that, “..since the matter is subjudice in the Supreme Court of India, the suggestion to have a judicial member may await the decision of the SC.”<sup>52</sup> It was desirable that the legislature should have dealt with this in great detail, as the majority of the stakeholders who have submitted their views have tilted towards a judicial member in the CCI.

- IPR defence for abuse of dominance: The Competition Act does not have an IPR defence in cases of section 4, unlike section 3. The CLRC, in its report, recommended that a defence allowing reasonable conditions protecting IPR may be provided for abuse of dominance cases.<sup>53</sup> The Draft Competition (Amendment) Bill, 2020, proposed the insertion of section 4A, providing a defence for abuse of dominance cases. The SCF, in its report, also proposed the insertion of section 4(3), providing a defence allowing reasonable conditions protecting IPR in cases of abuse of dominance.<sup>54</sup> However, the Amendment Act, 2023, did not incorporate this amendment.

The Competition (Amendment) Act, 2023, apart from above mentioned lacunas, has comprehensively addressed the regulatory gaps and will help CCI to respond effectively to the changing business environment in India.

---

<sup>52</sup> *Supra* note 5 at 50.

<sup>53</sup> *Supra* note 3 at 114.

<sup>54</sup> *Supra* note 5 at 54.

## **EMPOWERING CLEAN ENERGY: LEGAL PATHWAYS TO RENEWABLE ENERGY ADOPTION IN INDIA**

Snigdha Sharma\*

Nikhil Sharma\*\*

---

### **ABSTRACT**

India being among the fast-growing economies in the world is faced with the twin challenge of meeting its growing energy demand and protecting the environmental sustainability. In this regard, transition to renewable energy has been considered as a critical direction, and the legal framework has been identified as the core player in influencing this direction. This paper examines how the legal and regulatory framework in India is contributing towards its path towards more sustainable and environmentally friendly energy environment.

The study examines constitutional provisions including Article 48A and Article 51A(g) to emphasize the significance of environmental conservation and some of the important legislations like the Electricity Act, 2003, the National Electricity Policy, and the proposed Renewable Energy Act. It also evaluates the role played by institutions such as the Ministry of new and Renewable Energy (MNRE) and the Central Electricity Regulatory Commission (CERC) in the development of important policy instruments such as renewable Purchase Obligations (RPOs), feed-in tariffs and open access frameworks.

The paper shows major judicial pronouncements, which have influenced the lines of the energy law and environmental jurisprudence in India. It provides strategic advice that may be utilized to address the faults and gaps in the legal system to improve legal certainty, investor confidence, and inclusive energy access by identifying the gaps and strengths of the legal system. Finally, it assumes that an effective dynamic legal framework, which is well enforced, is key to accelerating the energy transition in India and achieving their domestic and international climate commitments.

**Keywords:** Renewable Energy, Legal Framework, Environmental Sustainability, Energy Policy, Climate Goals

---

\* LLM Student, Chandigarh university, Mohali, Punjab

\*\* LLM Student, Chandigarh university, Mohali, Punjab

## **1. Introduction**

India is also one of fastest growing economies in the world, and therefore, it finds itself in a crossroads in trying to balance its surging energy demand and the urgent environmental impacts.<sup>1</sup> As much of the energy consumption is expected to be more than doubled by 2040, being on the brink of decision making between the economic development and environmental sustainability, the country has a pressing task in front of itself.<sup>2</sup> At the same time, India has become vulnerable to climate-related risks, such as temperature increase, unpredictable weather, and water stress, which requires a certain shift toward a more sustainable and climate-neutral energy system.

The transition to the renewable energy is not a just policy issue but a legal must in the quest to have a sustainable future.<sup>3</sup> Commitments made by India in international treaties such as the Paris Accord and the country specific Nationally Determined Contribution (NDC) mean that the need to have a legal ecosystem in place that not only enhances but also, in an active way, drives clean energy deployment is fundamental.<sup>4</sup> Policies and regulations must be consistent, transparent and have enforceability to entice investments, maintain a welfare of the people, and maintain equal access to green energy.

Legal change cannot be effective unless it is more than a sectoral adjustment. They should also be holistic and should involve environmental protection, economic and social fairness. The legal instruments are to not only ensure the phasing out of carbon-intensive systems but also support innovation and guard the rights of the communities and the ecosystems.<sup>5</sup> The current legal frameworks must be revised and harmonized to get rid of inefficiencies and contradictions. In the end, prospective and holistic approach to legal policy is the key to achieving the untapped Indian potential in renewable energy.

## **2. A Legal Basis of Green Growth: Constitutional Mandates**

Although it was evident that when the Indian constitution was originally designed the institutionalization of environmental protection was not its primary agenda, it has come to

---

<sup>1</sup> International Energy Agency, *India Energy Outlook 2021* (IEA 2021) <https://www.iea.org/reports/india-energy-outlook-2021> accessed 11 July 2025.

<sup>2</sup> International Energy Agency, *India Energy Outlook 2021* (IEA, 2021).

<sup>3</sup> Shibani Ghosh, 'Laws for the Clean Energy Transition in India' (Centre for Policy Research, 2020) <https://cprindia.org/research/reports/laws-for-clean-energy-transition> accessed 11 July 2025.

<sup>4</sup> UNFCCC, *India's Nationally Determined Contributions* (submitted 2 October 2016) <https://unfccc.int/sites/default/files/NDC/2016-10/India%20First%20NDC.pdf> accessed 11 July 2025.

<sup>5</sup> World Resources Institute (WRI), *Enabling Clean Energy Investments in India* (2020) <https://www.wri.org> accessed 11 July 2025.

assume a highly level playing field in its subsequent development in the provision of the legislation regarding the environmental protection and the development of clean energy. This changed with the passing of the 42nd Constitutional Amendment in the year 1976 that brought with its article 48A and Article 51A(g). The Directive Principles of State Policy in article 48A imposes a duty upon the State to conserve, boost, and ameliorate the environment and protect the natural resources available in the country. In line with this, Article 51A(g) entrenches a kind of duty that citizens must conserve and improve their natural environments, such as forests, rivers and wildlife.<sup>6</sup>

This framework is further reinforced by Article 21 of the constitution which preserves the basic right to life and personal liberty. By a series of judicial interpretations, such a right has evolved to achieve environmental rights, including the right to a clean, healthy, and sustainable environment. In such landmark cases as *Subhash Kumar v. State of Bihar*<sup>7</sup> and *M.C. Mehta v. Union of India*,<sup>8</sup> the Supreme Court upheld environmental protection as a part of the right to life and thus enshrined the right of environment in Indian constitutional order.

All these constitutional provisions enable the legislature, executive and the judiciary to be proactive in promoting sustainability in the environment. They not only act as guiding principles but are binding requirements that have been used to spur both the number of public interest litigation and policy making on the behalf of renewable energy and environmental protection. This synergy of articles 48A, 51A (g) and 21 has already provided a strong legal framework to the transformation of India towards a green and a more sustainable energy path.<sup>9</sup>

### **3. Legislative Landscape: Powering Progress**

#### **3.1 The Electricity Act, 2003**

The legislative system of India has a big role towards transforming the country into renewable sources of energy. The nucleus of this terrain is the Electricity Act, 2003, being a landmark legislation which reorganized the power sector of India by introducing competition and transparency in it and pushing forward the aspect of renewed sources of power. Section 86(1)(e) of the Act requires State Electricity Regulatory Commissions (SERCs) to facilitate cogeneration and the generation of electricity with renewable energy sources by making

---

<sup>6</sup> Constitution of India 1950, arts 48A and 51A(g) (inserted by the Constitution (Forty-second Amendment) Act 1976).

<sup>7</sup> *Subhash Kumar v. State of Bihar* AIR 1991 SC 420.

<sup>8</sup> *M.C. Mehta v. Union of India* 1987 SCC 395.

<sup>9</sup> Shibani Ghosh, 'Laws for the Clean Energy Transition in India' (Centre for Policy Research, 2020) <https://cprindia.org/research/reports/laws-for-clean-energy-transition> accessed 11 July 2025.

appropriate connectivity arrangement to the grid and by the sale of such electricity to any person, and also the manner in which Renewable Purchase Obligations (RPOs) are to be stipulated on distribution licensees.<sup>10</sup> This provision of legal obligation establishes a market demand of clean energy and becomes a driving force behind various renewable energy programs developed in different states.

### **3.2 National Electricity Policy & Tariff Policy**

In addition to the Electricity Act are two important policy documents which include the National Electricity Policy (2005) and the Tariff Policy (2006, 2016). The policies complement the requirement of the use of renewable energy by underlining preference tariffs, access of grid to renewables, and technology-neutral bid procedures. In 2016 the Tariff Policy was amended such that state governments must make sure a big proportion of their energy procurement is through renewable means.<sup>11</sup> Such instruments of policy are characterized as soft laws, and thus they give an orientation to the regulatory process and entice the private sector to engage in the clean energy sector.

### **3.3 Draft Renewable Energy Act**

The Ministry of New and Renewable Energy (MNRE) proposed the Draft Renewable Energy Act in 2015 as a means of realizing the necessity of a unified legal framework. The objective of the proposed Act is to establish a cohesive body of legislation to support all renewable energy programs through establishing national renewable energy targets, implementing compliance provisions and imposing fines in case of non-compliance.<sup>12</sup> The proposed legislation in its current draft form indicates that the government sees the need to shift a disjointed regulatory system to a coherent and enforced legislative framework. This type of law would reduce legal uncertainty, enhance the confidence of the investor, and maintain consistency among state-based energy regimes.

The combination of these two legislative actions can be seen as a step in the progressive effort of readjusting India to sustainability in energy focus. Nevertheless, they have low efficacy and rely strongly on implementation, enforcement, and uniformity of regulations, and consistency of state and central government policies. With its current legal reforms, once passed and strictly

---

<sup>10</sup> Electricity Act 2003, s 86(1)(e).

<sup>11</sup> Ministry of Power, *National Electricity Policy 2005; Tariff Policy 2006 (amended 2016)* (Government of India) <https://powermin.gov.in/en/content/national-electricity-policy> accessed 11 July 2025.

<sup>12</sup> Ministry of New and Renewable Energy (MNRE), *Draft Renewable Energy Act 2015* <https://mnre.gov.in/file-manager/UserFiles/draft-renewable-energy-act-2015.pdf> accessed 11 July 2025.

followed up, it can carry out a paradigm shift towards popularization of renewable energy in the Indian power sector.<sup>13</sup>

#### **4. Regulatory Institutions: Forming the Clean Energy Ecosystem**

Successful renewable energy transition in India cannot just rely on legislative frameworks alone, but it also relies on the effectiveness and strength of regulatory institutions that serve to operationalise any given framework. These institutions at the centrally, as well as state-level, is instrumental in the implementation of policies, the structure of incentives and implementation of regulatory measures thus creating a structural framework in the Indian clean energy outlook.

The Ministry of New and Renewable Energy (MNRE) is the main central authority that has the responsibility of developing regimes in the form of policy and programmes in renewable energy. It develops national policies, spurs technological advancement, handles the international relations, and controls the allocation of financial subsidies like the capital subsidy and soft loans. The flagship programs such as the Rooftop Solar Programme and the PM-KUSUM scheme implemented by MNRE are specially designed to strengthen energy access and decentralised renewable systems.<sup>14</sup>

The Central Electricity Regulatory Commission (CERC) or several State Electricity Regulatory Commissions (SERCs) are also instrumental, in line with the MNRE. The responsibility of such quasi-judicial organizations rests on tariff decision, the implementation of Renewable Purchase Obligations (RPOs) and the provision of renewable energy producers with grid access. Even though the implementation of regulation has been performed successfully in certain states (especially Gujarat and Karnataka), the others ought to encounter some barriers like the institutional inertia of the state, uneven policy and regulation, and the lack of resources.<sup>15</sup> To provide confident grid connection of renewable energy, organizations, like the National Load Dispatch Centre (NLDC) and Regional Load Dispatch Centres (RLDCs) observe and control the energy circulation. These agencies play a central role of balancing the electricity demand

---

<sup>13</sup> UNFCCC, *India's Nationally Determined Contributions* (submitted 2 October 2016) <https://unfccc.int/sites/default/files/NDC/2016-10/India%20First%20NDC.pdf> accessed 11 July 2025.

<sup>14</sup> Ministry of New and Renewable Energy, *Annual Report 2022–23* (Government of India) <https://mnre.gov.in> accessed 11 July 2025.

<sup>15</sup> Prayas (Energy Group), 'Renewable Energy Regulation in India' (2021) <https://www.prayasgroup.org/peg/publications/item/511-renewable-energy-regulation-in-india.html> accessed 11 July 2025.

and supply since sources such as wind and solar are variable.<sup>16</sup> They are also increasingly taking the opportunity of forecasting technologies and energy storage mechanisms to do so.

Moreover, specialised agencies such as the solar Energy Corporation of India (SECI) and the Indian Renewable Energy Development agency (IREDA) have been supporting the sector by undertaking project development and financing. SECI enables competitive bidding of the large-scale solar and wind projects and signs Power Purchase Agreements (PPAs), and IREDA provides financing options to attract the government to fund private participation in renewable energy infrastructure.<sup>17</sup>

In spite of these developments, there are still issues. Some of these state regulatory agencies are still struggling with financial and administrative challenges, and this does not allow them to implement the policy requirements. In addition, differences in cross-jurisdictional trends of a regulatory interpretation and integration shake the confidence of investors and slow down the implementation of projects. To maximize the opportunity of the clean energy transition in India, these concerns should be considered by promoting the independence of institutions, the cooperation between institutions and capacity-building.<sup>18</sup>

## **5. Judicial Interventions: Green Guardians of the Courts**

Indian judicial system has been revolutionary when it came to the protection of environment and has indirectly made the switch to renewable energy. By successive interpretation of constitutional clauses and action in the cases of national interest issues, the courts have managed to take up an active position as the caretakers of environmental justice and sustainable development. The interpretation of Article 21 of Indian Constitution providing the right to life that is expected to be of major importance to the judiciary is the broad reading given to the provision. In the case the Supreme Court declared that right to life encompasses the right to breathe unpolluted air and drink pure water, and environmental rights became part and parcel of fundamental rights.<sup>19</sup>

On the same note, in *M.C. Mehta v. Union of India* the Court addressed the problem of industrial pollution and supported the principle of sustainable development ordering the State

---

<sup>16</sup> Central Electricity Authority, *Report on Renewable Energy Integration* (CEA 2022) <https://cea.nic.in> accessed 11 July 2025.

<sup>17</sup> Solar Energy Corporation of India (SECI), *About SECI* <https://www.seci.co.in> accessed 11 July 2025; Indian Renewable Energy Development Agency (IREDA), *Annual Report 2023* <https://www.ireda.in> accessed 11 July 2025.

<sup>18</sup> NITI Aayog, 'Power Sector Reforms in India: Toward a Resilient Energy Future' (2022) <https://www.niti.gov.in> accessed 11 July 2025.

<sup>19</sup> *Subhash Kumar v State of Bihar* AIR 1991 SC 420.

to find a balance between economic growth and environmental conservation. Such evolutions have informed the legal basis, through which environmental and energy policies have been developed, particularly those policies that exhibit preference in renewable sources as opposed to fossil fuels. Deliberations have not been restricted to interpretative functions of the judicial interventions.

In the case, the Supreme Court passed continuous, far-reaching directions to preserve the forest resources because of the ecological foundations of the long-term energy security.<sup>20</sup> These courses have assisted in making environmental conservation go hand in hand with energy law.

More to the point, certain renewable energy requirements have been successfully defended by courts. The Rajasthan High Court upheld the application of Renewable Purchase Obligations (RPOs) even on captive power generators and thereby held that the legislative instruments adopted to resolve the unutilised renewable resources problem are binding in nature.<sup>21</sup> In addition, the Public Interest Litigations (PILs) have also enabled citizens to voice their concerns regarding the issue of environmental depreciation and the failures in the energy policy, where the actions of the executive have been proven inadequate, and thus, the judiciary was inclined to act upon it. This has enhanced the system of accountability required in climate governance and regulatory compliance.

Despite the ongoing difficulties which include lack of enforcement and jurisdictional conflicts, the Indian judiciary remains a decisive power in creating a more environmentally friendly legal system as well as an energy system. Its proactive frame of reference casts an emphasis on the importance of an overarching legal strategy, which unites the principles of environmental justice with the efforts to establish clean energy sources.

## **6. Compliance and Policy: Legal and Policy Requisites on the Road to Clean Energy**

The legal and institutional frame of the renewable energy in India is strong on paper, but the actual practice grounded by serious obstacles. Such pressures are because of the existence of small procedural steps, sluggish administration, budgetary restrictions, and variation between different jurisdictions, which impacts negatively on a smooth implementation of clean energy programs.

---

<sup>20</sup> *T.N. Goda Varman Thirumulpad v. Union of India* 1997 SCC 267.

<sup>21</sup> *Hindustan Zinc Ltd. v. Rajasthan Electricity Regulatory Commission* 2015 SCC 1352.

The key undermining factor is the bogus implementation of Renewable Purchase Obligations (RPOs). As RPOs are prescribed by Electricity Act, 2003, and supported with national tariff policies, some states are short of meeting the target. Moreover, the policy is not well enforced, and the lack of strong punishment has diminished the effectiveness of the policy in creating demand of renewable sources of energy.<sup>22</sup>

Regulatory fragmentation is another on-going problem. Because of the difference in rules between states and the lack of harmonisation with central policies, policy uncertainty has emerged. The developers are often subject to delay in getting clearances, un-uniform tariffs, and ambiguous grid access procedures. Such regulation will deter investment in the private sector and make slow the rate of adoption of clean energy.<sup>23</sup> Land acquisition is one of the most time consuming and legally challenging parts of renewable project development. Solar and wind plants usually cover large spaces of land and land acquisition faces multiple hurdles in form of ownership, environmental permits, and local community opposition specially in forested and tribal lands.

Also, the financial woes of power distribution companies (DISCOMs) have distant repercussions in the renewable energy industry. Most DISCOMs withhold payment to energy producers and are reluctant to enter into Long-Term Power Purchase Agreements (PPAs) due to a lack of financial resources and efficiency to meet payment deadlines.<sup>24</sup> This economic insecurity scares away investors and destabilises the sector.

Aggravating all these factors is the small institutional capacity, particularly on state-level. Most regulatory agencies cannot appropriately adopt and enforce net-metering, open-access and consumer incentive policies of rooftop solar energy due to lack of human resources, technology to administer the same, and autonomy.<sup>25</sup> This makes the process of implementation still erratic and imperfect.

## **7. Comparative Insights: Comparative Lessons: International Success Stories**

With India still gearing up its renewable energy-based laws and policies, learning about international leaders in the clean energy transformation can be of any practical guidance.

---

<sup>22</sup> Prayas (Energy Group), 'Renewable Energy Regulation in India' (2021) <https://www.prayasgroup.org/peg/publications/item/511-renewable-energy-regulation-in-india.html> accessed 11 July 2025.

<sup>23</sup> Council on Energy, Environment and Water (CEEW), 'Mapping India's Renewable Energy Policy Landscape' (2022) <https://www.ceew.in> accessed 11 July 2025.

<sup>24</sup> The Energy and Resources Institute (TERI), 'Challenges in Renewable Energy Deployment in India' (2021) <https://www.teriin.org> accessed 11 July 2025.

<sup>25</sup> NITI Aayog, 'Report on Power Distribution Sector Reforms' (2022).

Countries like Germany, Denmark, and the United States have developed solid legal structures that have helped them to grow renewable energy at an alarming rate. These models evidence the effectiveness of well-designed policy laws, tax incentives, subnational governance, and participation of citizens to speed up integration of sustainable energy.

### **7.1 Germany: Ensuring Legal Stability and Investor Confidence**

The Energiewende of Germany can mainly be attributed to its Renewable Energy Sources Act (EEG). This legislation proposed feed-in tariffs (FiTs) to provide predictable pricing and long term to producers of renewable energy. The EEG promoted individual investment, cooperative and business investment by lessening the mystery of money. Additionally, robust planning policies and information sharing approaches practiced in Germany enabled the inclusion of renewables into the national grid without encountering much bewilderment and interference.<sup>26</sup>

### **7.2 Denmark: Empowering Local Communities through Law**

Denmark has promoted a bottom-up approach to the development of clean energy. Its legal framework requires the local communities to be provided with the chance to invest in and co-own the wind energy projects. The stable policies and regional planning laws have also contributed to great public support and trust to this participatory model. Consequently, more than half of the Danish power throughout is wind-generated. One of the legal milestones in the coordination and inclusive energy planning is the 2012 Energy Agreement.<sup>27</sup>

### **7.3 United States: Innovation within a Federal Legal Structure**

The contrasting but informative example here is provided by the United States, the state-level autonomy in a federal country has given a chance to legal innovation. Other states, such as California and Texas have adopted more liberal renewable energy legislation even without any federal rules. Examples of how subnational policies can establish ambitious clean energy targets include California Renewables Portfolio Standard (RPS) and carbon pricing. On the federal side, ITC and PTC are already aiding to decrease the prices of clean energy technologies, encouraging their popularization.<sup>28</sup>

### **7.4 Key Takeaways for India**

The developments in these countries include some of the lessons of importance to India:

---

<sup>26</sup> Bundesministerium für Wirtschaft und Energie, 'The Renewable Energy Sources Act (EEG)' (Germany, 2017) <https://www.bmwi.de/Redaktion/EN/Dossier/renewable-energy.html> accessed 11 July 2025.

<sup>27</sup> Danish Ministry of Climate, Energy and Utilities, 'Energy Agreement 2012 and Beyond' <https://en.efkm.dk> accessed 11 July 2025.

<sup>28</sup> U.S. Department of Energy, 'Renewable Electricity Production Tax Credit (PTC)' and 'Investment Tax Credit (ITC)' <https://www.energy.gov/savings> accessed 11 July 2025.

- Clear legal regimes are crucial to bring about the desired private investment.
- Locally owned by community and involving local people will result in enhanced acceptance by people and implementation.
- Fiscal rewards provided by legislation facilitate the competitiveness of renewable energy in front of conventional sources.
- Accountability and defined enforcement are provided by independent regulatory institutions.
- Centre-state initiative is important to prevent the fragmented policy implementation that is likely to prevail in a federal democracy.
- It can reinforce renewable energy transition in India by adopting and adapting these international best practices to the local context and making legal reforms effective and inclusive.

## **8. Recommendations: Strengthening Legal Pathways for Clean Energy**

The shift of India towards renewable energy does not only need inputs in the areas of technology and finance but it also will need a strong legal framework. A complex of specific legal and institutional changes is needed to address gaps in the existing regulatory framework and match it with the global climate goals.

1. **Codify a Unified Renewable Energy Legislation:** The existing law is scattered in several pieces of law and has not included binding requirements. A comprehensive Renewable Energy Act would bring together the detailed policies on a single legal framework. This Act is expected to set binding targets on renewable energy, institutional roles, and a provision on enforcement based on environmental justice and social inclusion.<sup>29</sup>
2. **Enhance the Capacity of Regulatory Bodies:** Both central and state level electric regulatory commissions need to be strengthened to make electricity regulation effective and consistent. The latter encompasses this with increased autonomy, technical training, digital tools to control regulation, and improved inter-state mechanism of coordination.<sup>30</sup>

---

<sup>29</sup> Ministry of New and Renewable Energy (MNRE), *Draft Renewable Energy Act 2015* <https://mnre.gov.in/file-manager/UserFiles/draft-renewable-energy-act-2015.pdf> accessed 11 July 2025.

<sup>30</sup> Prayas (Energy Group), 'Renewable Energy Regulation in India' (2021) <https://www.prayaspune.org/peg/publications/item/511-renewable-energy-regulation-in-india.html> accessed 11 July 2025.

3. **Establish Oversight and Accountability Mechanisms:** The transparency and accountability can be facilitated by introducing a statutory body or tribunal focused on the compliance with renewable energy. Tones that should be institutionalised are such mechanisms as judicial review of the regulatory decisions, fast-track of the project delays, and the review of the RPO compliance.<sup>31</sup>
4. **Facilitate Land and Infrastructure Access:** The case of renewable energy is scaled by land acquisitions and grid connectivity. It should include reforming this by using community consultation, transparent pricing, and environmental protection to facilitate these processes and as well require that they must be connected to the grid quickly.<sup>32</sup>
5. **Ensure Uniform Implementation of Open Access and RPOs:** The regulations of an open access and the RPO requirements are not uniform in states. There should be a centrally coordinated model regulation that can be adopted to create standard procedures and penalties of failure to comply to enhance certainty levels of the private investors and promote fair competition in the markets.<sup>33</sup>
6. **Incentivise Clean Energy Innovation:** There should be legal instruments that need to be developed to support the development of innovative technologies (like green hydrogen, offshore wind, and battery storage). Policies such as tax incentives, trading of carbon credits, and regulatory sandboxes should speed up its implementation and help in India achieving their carbon-neutral goals.<sup>34</sup>

## **9. Conclusion**

Clean energy future of India is not limited only to the technology and the fund but also to the vision and adaptability of the legal framework. The legal system will have its turn to respond to the momentous challenge of helping the nation realize its renewable energy ambitions and it will not be in the role of a mere structure, but that of a moving force that actively influences and helps this change.

What is needed is more than subtle reforms in the legal sphere. It demands the change in legal reasoning based on which sustainability will be one of the central values of governance, and access to clean energy will be understood as an essential element of development. The

---

<sup>31</sup> National Green Tribunal Act 2010; see also Centre for Science and Environment, 'Strengthening Environmental Governance in India' (2022).

<sup>32</sup> The Energy and Resources Institute (TERI), 'Land Acquisition for Renewable Energy Projects' (2021).

<sup>33</sup> NITI Aayog, 'Power Sector Reforms in India: Toward a Resilient Energy Future' (2022) <https://www.niti.gov.in> accessed 11 July 2025.

<sup>34</sup> International Renewable Energy Agency (IRENA), 'Innovation Landscape Briefs' (2023) <https://www.irena.org> accessed 11 July 2025.

innovating legal regime should ensure future predictability to the investor, responsibilities within the institutions, safeguard communities, and ecosystems that may be affected by the energy transition.

The law can be a force of change when it is done right and when carefully considered, it can help India have an energy future that is encompassing, sustainable and ecologically fair. The path is not simple, but with proper legal instruments, India can show the rest of the world how the economic growth and environmental sustainability can be compatible. The winds of change are blowing, and it is the law that has to continue the journey.

**Geeta Institute of Law  
Panipat, Haryana, India**

**Volume 14(1)**

**June 2025**