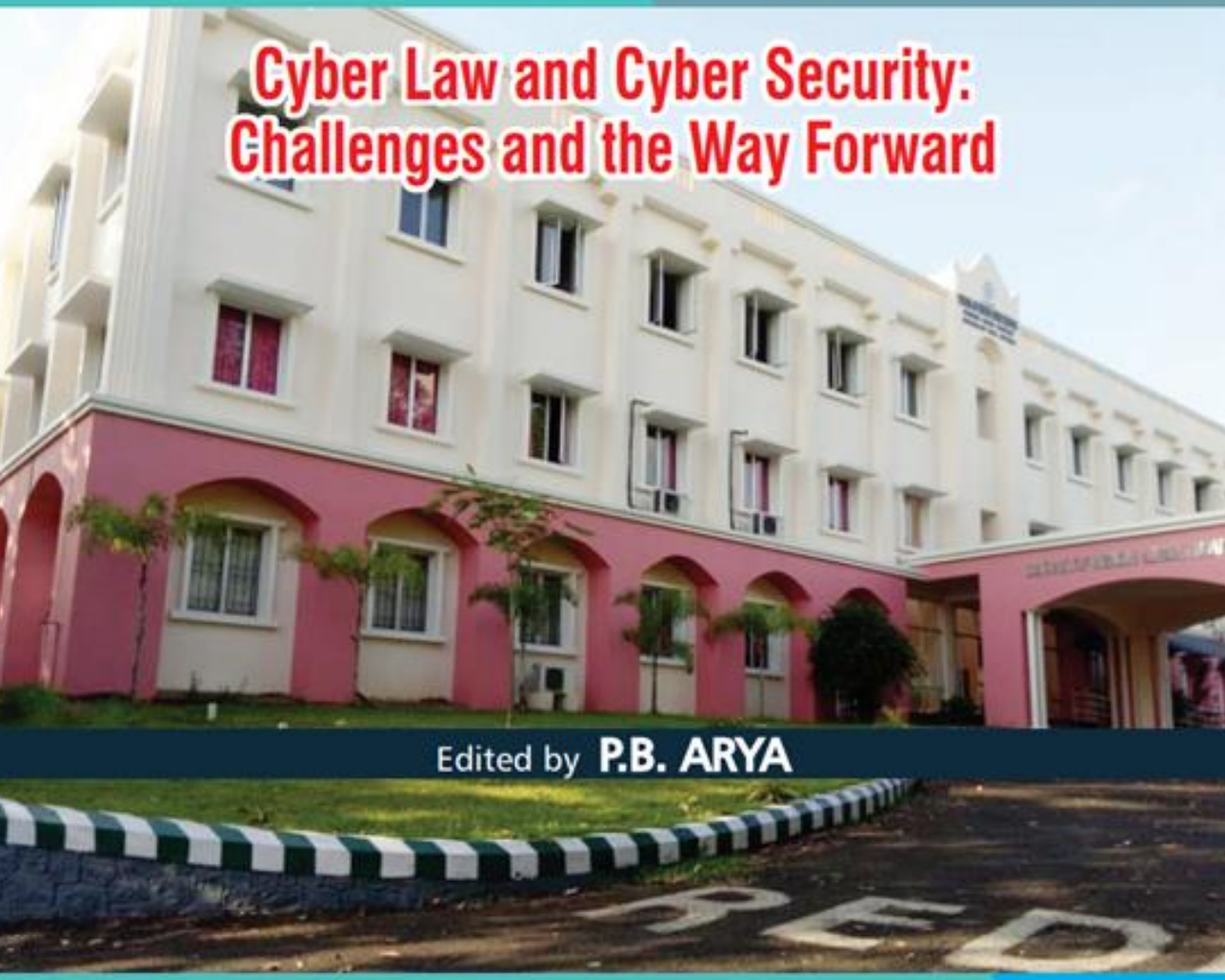
# Cyber Law and Cyber Security: Challenges and the Way Forward



Edited by **P.B. ARYA**


School of Indian Legal Thought
Mahatma Gandhi University
Kottayam, Kerala

Book
**Cyber Law and Cyber Security:**
**Challenges and the Way Forward**
(English)

ISBN 978-93-80419-767-3

*Editor*

**P.B. Arya**
*Assistant Professor, School of Indian Legal Thought,*
*MG University, Nattassery, Kottayam*

*Student Editors*

**Reneeta Vinu**
**Anagha K. Ayriyil**
**Sreenarayani J. Menon**
**Vishnupriya T.V.**

Printed in India at alenlayout, Manganam, INDIA. Ph: 9446859012

# Preface

The School of Indian Legal Thought (SILT) at Mahatma Gandhi University was established with the objective to offer comprehensive legal education through distinctive programs designed for undergraduate, postgraduate, and research levels. The School has been organising seminars/ conferences, workshops, colloquia and other academic activities with the objective to provide a point of convergence for lawmakers, academicians, and the general public. The School of Indian Legal Thought had organised a Two Day National Seminar on 'Cyber Law and Cyber Security – Challenges and the Way Forward' on 3rd and 4th March, 2023 to discuss the major issues in the field of cyber law and the legal challenges posed by the advancing technologies.

With the exponential growth in the use of cyberspace, there has been a simultaneous flare-up of legal and other issues in relation to its usage. This book attempts to analyze the emerging trends, issues, and aspects pertaining to cyberspace in the present socio-legal context. The need to protect data privacy has recently been highlighted with the introduction of the Digital Data Protection Bill, 2022, and the efficacy of the Bill to address the data protection concerns is largely under discussion. At the same time the Information Technology Act, 2000 is criticized for being outdated and the need has been largely raised to replace this Act with new legislation. Unfortunately, statistics show that cybercrime has increased dramatically in the last three years, particularly in the post-covid times. Also significant is the large-scale impact the cybercrimes could have on the socio-economic milieu of the country, as is evident from the acts of cyber-warfare and cyber-terrorism. In this scenario there is a need to stimulate a revitalized and knowledge-based discussion of emerging issues in cyber law and cyber security.

This book is a collection of research articles which reflects the emerging legal concerns in the arena of cyber law. These articles are sure to enhance the current legal understanding on various issues of importance in cyber law and information technology. I hope these articles would provide the necessary platform for further research and discussions in these areas.

**P.B. Arya**

# CONTENT

# E-Commerce and the right to be forgotten in India; How Friend-user are the technologies offered by the Digital enterprise

*Ochieng fanuel mwamlenga*[1]

## Introduction

The fuel for the 'digital economy'[2] and business is data. Data is being harvested online on an unprecedented scale. Digital enterprises involved in this practice are thus quite active in collecting all sorts of data through pervasive techniques that track and collect huge amounts of information[3]. To ensure their targets are effective, these digital enterprises offer online technologies from which at the beginning appears to be easy for the 'data principals'[4] to feed in their personal data once they want to access services

1 Sub-theme: Cyber Law and Data Privacy. Phone Number: +91 8891590612; E-mail Address: ochiengfanuel6232@gmail.com

2 The digital economy refers to a broad range of economic activities that use digitized information and knowledge as key factors of production. The internet, cloud computing, big data, fintech, and other new digital technologies are used to collect, store, analyze, and share information digitally and transform social interactions. Accessed on 27/01/2023 through https://www.adb.org/news/events/understanding-digital-economy-what-it-and-how-can-it-transform-asia.

3 ELIF K. CORTEZ, DATA PROTECTION AROUND THE WORLD: Privacy Laws in Action, 249 [AsserPress 2021].

4 "Data Principal" refers to the individual to whom the personal data relates and where such an individual is a child includes parents or lawful guardians of such a child.

provided by these companies but these technologies are too sophisticated and technically not 'User-Friend' to the data principals whenever they want to withdraw their consents and/or exercise their right to be forgotten.

Thus, this practice has drastic consequences for the privacy and the security of such data. This presumption leads down to the hypothesis of this research that; the failure of these enterprises to provide Use-Friend technologies that could enable the data principals to withdraw their consents and exercise their right to be forgotten whenever they want influences the manipulation of the data collected by these companies eventually might lead to unforeseeable consequences to the data principals.

Therefore, firstly, in this study we are going to elucidate the meaning and the scope of the concept of the right to be forgotten. Secondly, we will discuss the applicability of the right to be forgotten in relation to technologies employed by these enterprises (i.e. Websites, Applications, cookies, Terms of Use etc) for tracking and targeting the data principals in processing data while assessing the effectiveness of the technologies offered by the digital enterprises in complying with the right to be forgotten. And finally, this study will assess the consequences of the technologies deployed by these digital enterprises over the protection and securing the privacy of users.

## E-commerce Trends in India

India has the third-largest online shoppers base globally, in 2021 it ranged between 180-190 Million shoppers and is expected to rise to 450-500 Million by 2030. Currently, there are more than 19,000+ E-commerce companies in India. The Indian E-commerce companies and their market would increase from USD 38.5 billion in 2017 to USD 200 billion in 2026[5]. The big 5 are Amazon, Flipkart, Myntra, IndiaMART and Shopclues.

5 BT BUSINESS TODAY, https://www.businesstoday.in/latest/economy/story/india-has-the-third-largest-online-shopper-base-globall y-to-overtake-us-in-1-2-yrs-bain-co-349631-2022-10-12 [last accessed on 21st February 2023].

## The Right to be Forgotten

Refers to the right of an individual to either delete, limit the disclosure or direct the use of his/her personal information on the internet, which is misleading, embarrassing, irrelevant, outdated or as the exercise of withdrawal of his/her consent. Such disclosure may or may not be a consequence of unlawful processing by the data fiduciary[6]. The right to be forgotten insists on one's personal information to be removed from the online sources which are available and/or can be accessible to the public such as, search engines or other online platforms[7].

The right to be forgotten is also sometimes referred to as the right to erasure[8]. Despite the term 'right to be forgotten' sometimes being used interchangeably with the term 'right to erasure' there is an intrinsic difference between the two. The 'right to erasure' requires the deletion of the data from the very main source where the respective data was stored, while on the other hand, according to the 'Srikrishna committee"[9], the right to be forgotten should not extend to the right to erasure rather the disclosure of such data can be curtailed if some conditions are satisfied[10]. These conditions may include but not limited to the exercise of the Right to freedom of expression and information, fulfillment of legal responsibilities, execution of a duty in the public interest or public health, protection of information in the public interest, for the purpose of scientific or historical study, or for statistical

6 RSTV, https://www.youtube.com/watch?v=XN5HbVhcuq4&t=3s accessed on 18th January 2023.

7 Right to be Forgotten: https://www.drishtiias.com/daily-updates/daily-news-analysis/right-to-be-forgotten-6 [accessed on 16th March 2023].

8 GDPR.EU, Everything you need to know about "the right to be forgotten": https://gdpr.eu/right-to-be-forgotten/ [accessed on 21st February 2023].

9 The Committee was appointed by the Ministry of Electronics and Information in 2017 to submit a report on Privacy and a Draft Personal Data Protection Bill.

10 Sohini Chatterjee through RStv: https://www.youtube.com/watch?v=XN5HbVhcuq4&t=3s [accessed on 18th January 2023].

purposes or the establishment, executing, or defending of legal claims[11]. This signifies that the right to be forgotten is not entirely absolute, it is subject to reasonable limitations.

## The Right to be Forgotten in the European Union

The right started in 2014 by the EU court of Justice in the case of Google Spain v. Mario Costeja Gonzalez[12]. In 1998, Mario Costeja Gonzalez had undergone bankruptcy and was facing financial difficulties. Hence, he decided to put his property for auction in the advertisement through the newspaper, and the advertisement aws taken to the internet without his prior knowledge and it stayed there permanently. For a long time, he was considered bankrupt because the information about the sale of his property was accessible to the public all alone in the google search engines. Thus, it caused him severe damage to his reputation, hence prompted him to take up the matter to the court[13]. The main issue in this case was to determine whether the records of past convictions can be removed from the search engine. Google Spain argued the defendant has no right to erasure, and the Attorney General propounded that the right to privacy cannot supersede the right of the public to know. In its decision in 2014, the European Union court of Justice upheld the right to erasure where it provided that "..the search engine operator is responsible for the processing of the personal data uploaded in their website by the third party."[14]

Later the right to be forgotten was incorporated in the EU General Data Protection Regulations in 2018 (hereinafter being referred as G.D.P.R 2018). In the European Union, the collection, processing, and the erasure of the personal data is regulated under GDPR, 2018[15].

11 MANUPATRA ARTICLES, https://articles.manupatra.com/article-details/Right-to-be-forgotten (accessed on 16th March 2023.)

12 Google Spain v Mario Costeja Gonzalez, EU-CJ, C-131/12.

13 MANUPATRA ARTICLES, supra note 10.

14 GOOGLE SPAIN, supra note 11.

15 GDPR.EU, supra note 7.

## The right to be Forgotten in India

The right to life and personal liberty[16] is the fundamental constitutional right which has laid the basic foundation for the protection of the 'right to be forgotten' in India. Currently in India there is no specific statutory legislation that regulates personal data protection thus the right to be forgotten in India is considered to be developed through judicial observations. At first it was recognized in the landmark constitutional bench case of Justice K.S Puttaswamy(Retd) and Ors

v. Union of India and Ors[17], when the court declared the right to privacy as a fundamental right under Article 21 Constitution of India and the right to be forgotten forms part of it. Specifically speaking for the right to be forgotten the court clearly observed that "..individuals should have the right to be forgotten" the court further added that "human beings forget but the internet never forgets". Right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution[18]. In Prem Shankar Shukla v. Delhi Administration[19] Justice Krishna Iyer, speaking observed that: "...the guarantee of human dignity, which forms part of our constitutional culture, and the positive provisions of Articles 14, 19 and 21 spring into action when we realize that to manacle man is more than to mortify him; it is to dehumanize him and, therefore, to violate his very personhood, too often using the mask of 'dangerousness' and security..."

In Sredharan T v. State Of Kerala[20] The Kerala High Court in this case recognized the 'Right to be forgotten' as a part of the Right to privacy. In

16 INDIA CONST. art. 7.

17 Justice K.S. Puttaswamy(Retd) and Ors v. Union of India And Ors, Writ petition (Civil) No. 494 of 2012, (2017) 10 SCC 1

18 DRISHTIIAS DAILY UPDATES, Right to be forgotten: https://www.drishtiias.com/daily-updates/daily-news-analysis/right-to-be-forgotten-6 [last visited on 14th March 2023].

19 MANU/SC/0084/1980.

20 Writ Petition No. 9478 of 2016.

this case, a writ petition was filed for protection of the Right to privacy under Art.21 of the constitution and petitioner was seeking directions from the court for the removal of the name and personal information of the rape victim from the search engines in order to protect her identity. The court held in favor of the petitioners recognizing the 'Right to be forgotten' and issued an interim order directing the search engine to remove the name of the petitioner from orders posted on its website until further orders were issued.

The Karnataka High Court in the case of Sri Vasunathan v. Registrar General[21], upheld a women's 'Right to be forgotten' and Justice Bypareddy had observed that "This is in line with the trend in western countries of the ''Right to be forgotten" in sensitive cases involving women in general and highly sensitive cases involving rape or affecting the modesty and reputation of the person concerned."

In the Zulfiqar Ahmad Khan v Quintillion Business Media Pvt. Ltd.[22], the Delhi High Court supported an individual's 'Right to be forgotten'. In that instance, Plaintiff petitioned the Hon'ble Court for a permanent injunction against the Defendants, who had authored two articles against Plaintiff based on harassment accusations they claimed to have received, as part of the #MeToo campaign. Even though the Defendants agreed to remove the news stories, they were reprinted by other websites in the meantime. The Court noted the Plaintiff's Right to privacy, of which the ''Right to be forgotten" and the 'Right to be Left Alone' are inbuilt aspects, and guided that any republishing of the content of the originally disputed articles, or any abstract therefrom, as well as altered forms thereof, on any print or digital/electronic platform be held back during the pendency of the current suit.

In Subranshu Raot v. State of Odisha[23] The Orissa High Court examined the 'Right to be forgotten' as a remedy for the victims of sexually explicit videos or photos often posted on social media for harassing the victims.

---

21 Writ Petition No.62038 of 2016.

22 CS (OS) 642/2018.

23 WP (C)/4159/2020

In 2018 the right to be forgotten was included into the recommendations of the Justice BN SriKrishna Committee which was appointed by the ministry of electronics and information in 2017 under the chairmanship of Justice BN Srikrishna, the committee was constituted with 10 members with the purpose to submit a detailed report on privacy and draft the Personal Data Protection Bill.

According to the Supreme Court in the case of Justice Puttaswamy, the right to be forgotten in India gains its roots from the right to privacy which is a fundamental right guaranteed under Article 21 of Constitution of India[24].

In the case of Jorawar Singh Mundy vs Union of India[25] We can see manipulation of individuals' information whereby the Hon'ble Court ordered the respondents (i.e. Google, Lex.in and Indian kanoon) to remove the judgment from their platforms till the further order from the court[26].

## Why do we need it and what exactly has to be forgotten?

It is important to have the right to be forgotten because sometimes on search engines when someone searches for something and personal data that relates to that search can easily pop up and be accessed by such person who searches and ultimately it might injure the reputation of the person to whom such data relates. Sometimes it might happen that a person may be accused of several offenses, and after the determination of the court such person found not guilty, but all the articles and materials that had been published on the internet about his accusations continue to be in the public domain. If he has been convicted of petty offenses there should be no need of his record to be detained and hunt him forever because primarily prisons are considered to be places for reformation from which the convicts are given chance to learn on how to become good citizens, thus such person after faithfully serving his terms in prison deserves to have another chance

24 DRISHTIIAS DAILY UPDATES, supra note 17.

25 MANU/DE/0954/2021.

26 MANUPATRA ARTICLES, supra note 10.

of being free from the shadows of the mischief he did previous. And if he/she was convicted of other offenses and served the sentence, then he/she shall not have a right of his data to be removed, but there should be a mechanism that will help him not to suffer from the stigma of what he did. In cases such as revenge porns and forced accusations, the reputation of the data principals are tarnished to an unimaginable and irreparable extent, thus in incidents like these there should not just be a right to be forgotten but the data should be deleted and removed permanently from all sources possible. So, in all the incidents above and others, the right to be forgotten will balance the essence of the right to privacy of an individual.

## When does the right to be forgotten apply?

Article 17 of the GDPR 2018 outlines the specific circumstances under which the right to be forgotten applies. An individual has the right to have their personal data erased if[27]:

- The personal data is no longer necessary for the purpose an organization originally collected or processed it.
- An organization is relying on an individual's consent as the lawful basis for processing the data and that individual withdraws their consent.
- An organization is relying on legitimate interests as its justification for processing an individual's data, the individual objects to this processing, and there is no overriding legitimate interest for the organization to continue with the processing.
- An organization is processing personal data for direct marketing purposes and the individual objects to this processing.
- An organization processed an individual's personal data unlawfully.
- An organization must erase personal data in order to comply with a legal ruling or obligation.

27 GDPR.EU, supra note 7.

- An organization has processed a child's personal data to offer their services without the consent of either parent or lawful guardian of that child.

## The Concept of Fiduciary and Data Ownership

When discussing the concept of fiduciary relating to data protection in India, it simply refers to the relationship of trust that exists between data principal and data fiduciary. According to the Digital Personal Data Protection Bill 2022[28], 'Data Principal' refers to the individual whose data is sought to be collected. While on the other hand, 'Data Fiduciary' refers to the service provider who determines the purpose and manner of data processing. In Augusta Mut. Ins. Co. v. Mason[29], it was observed that: "A fiduciary relationship exists in all cases when special confidence has been reposed in one who in good conscience is bound to act with due regard for the interest of the one reposing the confidence"[30]. Here 'trust' is the key element as fiduciary is merely considered to mean a person or an organization (i.e. that is in charge of processing or controlling management of personal data) that acts on behalf of 'data principal' to manage his or her personal data. In our case here, all E-commerce companies are covered under the armpit of this description[31]. According to Recitals 65 and 66 in Article 17 of the G.D.P.R 2018, the data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue influence. And in assessing what constitutes 'undue delay' it has to be at least about a month[32]. Data is shared for the particular purpose, and it has to be

28 The newly proposed bill by the Indian government to repress the previously proposed Data Protection Bill,2019.

29 Augusta Mut. Ins. Co. v. Mason, 274 Va. 199, 645 S.E.2d 290(2007).

30 BRIEN ROCHE LAW, https://www.brienrochelaw.com/tort-law/tort-case-law/f/fiduciary-duty/ [accessed on 18th January 2023.]

31 CITIZEN MATTERS, https://www.brienrochelaw.com/tort-law/tort-case-law/f/fiduciary-duty/ [last visited on 14th February 2023.

32 GDPR.EU, supra note 7.

used only for that purpose. Since just 'trust' is the only thing which is submitted by data principal to data fiduciary and 'data ownership' then 'data principal' must have control and autonomy over his or her shared data, the manner in which such data will be used, disclosed or shared to the third party (in case consented by 'data principal'). The data ownership by the data principals will be of no meaning if they will not have control over their data processing whenever they intend to withdraw their consent or when they consider there are errors in processing such data or the shared data are no longer relevant, continuing being held by data fiduciary.

## The concept of Informed Consent

Informed consent means a free express manifestation of the Data Principal's wishes which may either be by a statement or a clear affirmative action, signifying his consent to the collection, processing, retention, or disclosure of his/her Personal Data after receiving the sufficient knowledge about the data process from the intended data fiduciary. The data principal has a right to be informed of the purpose for which his data are collected or processed. Furthermore, he is entitled to know the security measures and other protection measures which the data fiduciary has in place to ensure confidentiality and integrity of the data. Equally, the data principal is entitled to know in advance whether his data will be shared with the third parties, the extent of such sharing and any necessary repercussions[33]. In the Facebook-Cambridge Analytica case, the Facebook owner Meta agreed to pay $725m (£600m) to settle legal action over a data breach linked to political consultancy Cambridge Analytica[34]. In this case Facebook exposed data on up to 87 million Facebook users without obtaining their official consent, to a researcher who worked at Cambridge Analytica[35].

33 ELIF K. CORTEZ, supra note 2 at 250-263.

34 BBC NEWS, https://www.bbc.com/news/technology-64075067 [accessed on 19th February 2023].

35 VOX, https://www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridge-analytica-trump-diagram accessed on 19th February 2023.

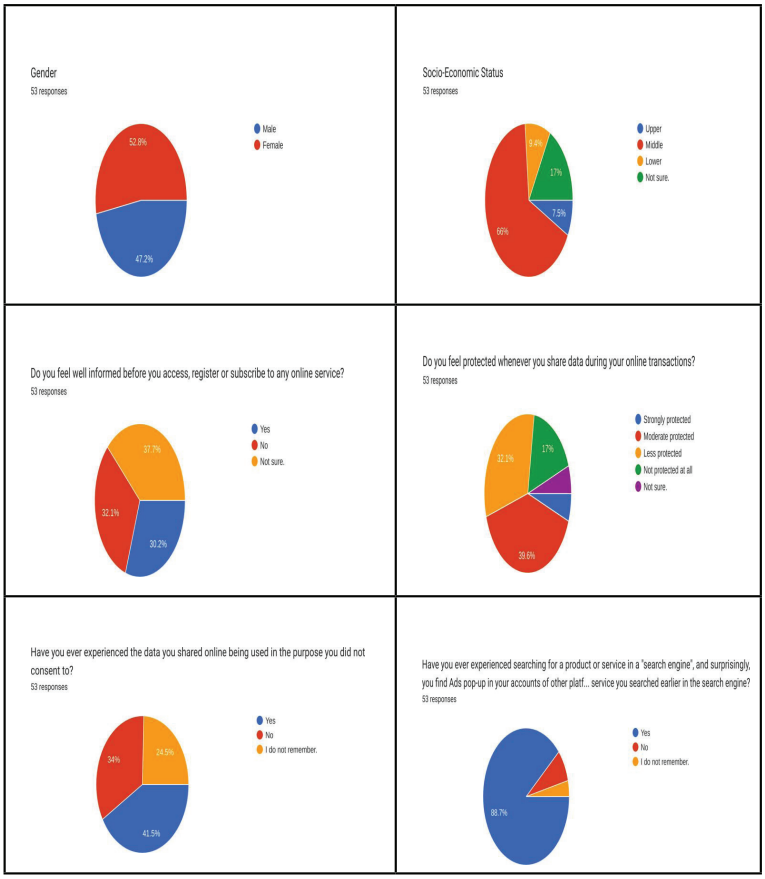
Technically, this right allows data principals to know what personal data is collected about them, why, who is collecting data, how long it will be kept, how they can file a complaint, and with whom they will share the data. During the process of data collection or processing, the following information are required to be provided to the data principals; the data fiduciary's information and contact details, purpose of data processing, legal basis for personal data processing, third party details in case data will be shared with the third party, data retention period, rights granted to the data subject under the data protection law, the right to file a complaint; and, whether the data principal has a legal obligation to provide personal data.[36]

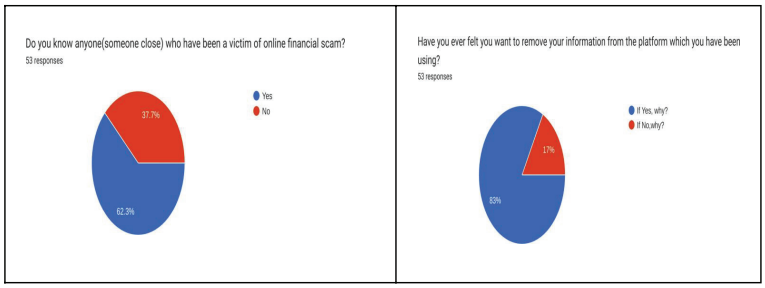
## Research Methodology

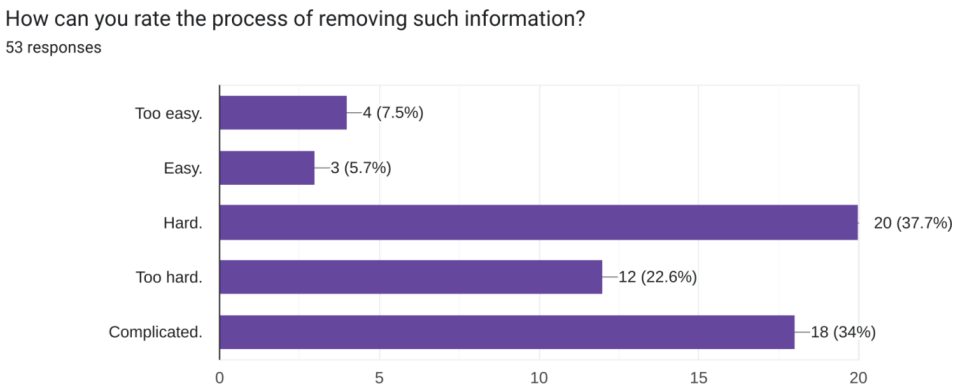
A simple study was conducted, an online questionnaire was circulated, and the responses were collected from around several states of India. The questionnaire included the demographic, introductory and the main questions. The researcher also used the Observation method as a tool of data collection.

***Sample of the Collected data assessing the experience of the data principles to the E-commerce and online platforms.***

36 ELIF K. CORTEZ, supra note 2 at 258-268.


Gender
53 responses
52.8%
47.2%
Male
Female
Socio-Economic Status
53 responses
9.4%
17%
7.5%
66%
Upper
Middle
Lower
Not sure.
Do you feel well informed before you access, register or subscribe to any online service?
53 responses
37.7%
32.1%
30.2%
Yes
No
Not sure.
Do you feel protected whenever you share data during your online transactions?
53 responses
32.1%
17%
39.6%
Strongly protected
Moderate protected
Less protected
Not protected at all
Not sure.
Have you ever experienced the data you shared online being used in the purpose you did not consent to?
53 responses
34%
24.5%
41.5%
Yes
No
I do not remember.
Have you ever experienced searching for a product or service in a "search engine", and surprisingly, you find Ads pop-up in your accounts of other platf... service you searched earlier in the search engine?
53 responses
88.7%
Yes
No
I do not remember.


Do you know anyone(someone close) who have been a victim of online financial scam?
53 responses
37.7%
62.3%
Yes
No
Have you ever felt you want to remove your information from the platform which you have been using?
53 responses
17%
83%
If Yes, why?
If No,why?




## Research Findings and Analysis

The proposed hypothesis was proved by the statistical analysis of the data collected. Positive correlation was discovered between sophisticated and complicated technologies and the technical denial of the right to be forgotten hence the manipulation of the data collected from the data principles.

This research shows that despite continuing using the services by the online platforms, the data principles neither feel well protected nor well informed about the use and the repercussion of their data which they share. Also, the research reveals that data principals are experiencing their data which they have shared in one purpose being used for another purpose without their informed consent for the change of the purpose. Moreover, it's common for the data principals to experience their searches in 'search engines' popping up in their other online platforms as the advertisements of the products or services relating to their previous searches in search engines. This undoubtedly these search engines share personal data of the data principals with the online trading companies from which they might have commercial interests once they enter into their platforms. This poses a great threat to the identification of the data principles as well as their sensitive personal data. Due to these threats, data principals have been feeling of removing their data which they have shared to these platforms once they

feel it's no longer necessary for them continuing being held by these platforms, this research shows that it has never being easy for data principals to exercise their right of withdrawing their consents since these platforms have no friend-user means to enable them to remove their information once needed.

Tools like 'Cookies' and 'Terms of Use' are the major techniques which are used by the digital platforms to manipulate and misappropriate the personal data which are shared to them. The use of "cookies" as the technique which is used to collect data from the data principle in exchange of access to the services. It is a "Must accept" option, in which if the principal does not accept then he/she will be denied access to the services.

"Informed consent" mandates data fiduciary to inform and issue all the details of the third parties to whom he is intending to share the collected data and the data principal has to consent before the data being shared to the third party. But these companies do not issue these details though they share the collected data to whom they call 'partners'.

In their platforms they issue terms and conditions mostly provides as 'Terms of Use' which requires data principal to accept ALL the conditions, if he/she is not agreeing with some of the conditions, "Take it, or leave it" kind of contract, then he/she will only have one option of not registering to the platform, eventually he cannot access services something which denies data principal the right to be included to access socio-economic services in the country.

"We reserved the right, at our own discretion, to change, modify, add or remove portions of these Terms of Use, at any time without any prior written notice to you."

This quotation has been taken from "Terms of Use" of one of the major E-commerce companies which is having its businesses operations and is used by the majority of the online buyers in India. If we critically look at this term, the data fiduciary has power to change and modify its 'terms of use' without either obtaining consent or informing data principals about such changes.

This 'term of use' shows that these companies detain data and once data are shared to them automatic, they assume the right of data ownership from the data principal, something which is very wrong, we should know that data principals are the sole owner of the shared data and they just render their 'trust' of their data relating to their previous consented terms. So, if these companies want to change their 'terms of use' they must inform the data principals about the same and should obtain new consent before making these new terms into application.

These 'Terms of Use' are technically formulated in a way that these platforms are collecting what can be called 'General consent' which does not fit to be considered as proper 'informed consent'.

## Conclusion and Recommendations

As we have already discussed previous, currently there is no specific statutory law in India that regulates privacy and personal data protection. The Information Technology Act, 2000 is main statutory legislation regulating cyber matters in India, through it, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 have been enacted to cover some principles regulating persona data protection, despite their existence, the effectiveness of these 'Rules' seem failing to cover all the aspects of personal data protection in the country.

According to rule 5(1)[37] These digital companies are required to obtain consent in writing from the data principals of their personal data regarding the purpose of usage before the collection of such data. This brings the necessity of the law to require these companies to obtain separate consents depending on the specific purpose from which they are collected, and the 'terms of use' should not be used to obtain what can be called 'general

37 The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

consent' from the data principals and the information collected shall be used for the purpose for which it has been collected.

The right to withdraw the consent by the data principal forms a fundamental base from which the right to be forgotten lies on, so it must be a mandatory to digital platforms to provide data principals with the option to withdraw their consent given earlier and this option should have a mechanism which operates as simple as collection of data is done[38]. To effect this, the platforms should provide 'access tools' from which data principals can issue their requests. For instance, under the G.D.P.R, 2018 there is a requirement for "right to erasure request form" must be provided by the data collector or controller to the data subjects.

The disclosure of any personal data by the data fiduciary to the third party shall be subject to the consent and prior permission obtained from the data principal, 'terms of use' and 'cookies' should not be a ground for the digital companies to manipulate data shared by the data principal and being shared technically without proper consent.

Other relevant things to be taken into considerations are such as; The needs to enact legislation so as to establish it as a statutory law; The need to change the perception that it is only applicable to the search engines; The need to widen the provisions of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011. The 'Terms of Use' and 'Cookies' should not be used as a tool to obtain 'general consent'. The consent to each relevant aspect should be obtained separately.

Mostly, the 'right to be forgotten' has been evoked against search engines only rather than the companies that hold such data. Therefore, it is the right time now to widen the scope and the coverage of the right to be forgotten from which it has to cut across all the platforms in which personal data are processed.

38 I'd at rule 5(5).

## Reference:

ELIF K. CORTEZ, DATA PROTECTION AROUND THE WORLD: Privacy Laws in Action, 249 [Asser Press 2021]. https://www.adb.org/news/events/understanding-digital-economy-what-it-and-how-can-it-transfo rm-asia Accessed on 27/01/2023.

BT BUSINESS TODAY, https://www.businesstoday.in/latest/economy/story/india-has-the-third-largest-online-shopper-bas e-globally-to-overtake-us-in-1-2-yrs-bain-co-349631-2022-10-12 [last accessed on 21st February 2023].

RSTV https://www.youtube.com/watch?v=XN5HbVhcuq4&t=3s[accessed on 18th January 2023.

Right to be Forgotten: https://www.drishtiias.com/daily-updates/daily-news-analysis/right-to-be-forgotten-6[accessed on 16th March 2023].

GDPR.EU,Everything you need to know about "the right to be forgotten": https://gdpr.eu/right-to-be-forgotten/ [accessed on 21st February 2023].

Sohini Chatterjee through RStv:https://www.youtube.com/watch?v=XN5HbVhcuq4&t=3s [accessed on 18th January 2023].

MANUPATRA ARTICLES,https://articles.manupatra.com/article-details/Right-to-be-forgotten [accessed on 16th March 2023.]

DRISHTIIAS DAILY UPDATES, Right to be forgotten: https://www.drishtiias.com/daily-updates/daily-news-analysis/right-to-be-forgotten-6 [last visited on 14th March 2023].

BRIEN ROCHE LAW, https://www.brienrochelaw.com/tort-law/tort-case-law/f/fiduciary-duty/ [accessed on 18th January 2023.]

CITIZEN MATTERS, https://www.brienrochelaw.com/tort-law/tort-case-law/f/fiduciary-duty/ [last visited on 14th February 2023.]

BBC NEWS, https://www.bbc.com/news/technology-64075067[accessed on 19th February 2023].

VOX, https://www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridge-analyt ica-trump-diagram[accessed on 19th February 2023.]

Google Spain v Mario Costeja Gonzalez, EU-CJ, C-131/12.

Justice K.S Puttaswamy(Retd) and Ors v. Union of India And Ors, Writ petition (Civil) No. 494 of 2012, (2017) 10 SCC 1

Prem Shankar Shukla v. Delhi Administration, MANU/SC/0084/1980.

Sredharan T v. State Of Kerala, Writ Petition No. 9478 of 2016.

Sri Vasunathan v. Registrar General, Writ Petition No.62038 of 2016.

Zulfiqar Ahmad Khan v Quintillion Business Media Pvt. Ltd. CS (OS) 642/2018.

Subranshu Raot v. State of Odisha, WP (C)/4159/2020.

Jorawar Singh Mundy vs Union of India, MANU/DE/0954/2021. Augusta Mut. Ins. Co. v. Mason, 274 Va. 199, 645 S.E.2d 290(2007). INDIA CONST. art. 7.

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011.

The European Union General Data Protection Regulation, 2018.

# The Personal Data Protection and Cyber Security in India: Ananalysis of Digital Personal Data Protection Bill, 2022

***Neethu George***[1]

## Abstract

*In this fast-phased world, the access and exchange of information including personal data havebecome easier and faster than ever, through the Internet. The projects like Digital India have caused the digitalization of the Indian economy and have made India the largest connected democracy in the world with over 760 million active Internet users and is expected to touch 1.2billion in the next coming years.*

*Knowingly and unknowingly individuals are providing their personal data online formulti-purposes, such as online shopping, entertainment, e-learning, and other goods and services.Moreover, social interactions are increasing day by day, especially on social media platforms, whichcreates a risk to privacy.*

*This paper critically analysis provisions of the Digital Personal Data Protection Bill with theright to privacy and cyber security in India. It also analyses the implications of the SupremeCourt's judgment on the Puttuswamy case, and also comparatively studies the data protectionlaws of other nations.*

1 Faculty of Law, School of Indian Legal Thought, MG University, Kottayam.

## Introduction

PERSONAL DATA[2] is information that relates to an identified or identifiable individual. These data are processed by the business as well as government entities for the goods and servicesdelivery. Preferences of individuals are identified by the processing of personal data which maybe useful for target advertising, customization, and developing recommendations and, in fact, processing personal data may also aid law enforcement.

However unchecked processing may have adverse implications for the privacy of individuals, which has been recognized as a fundamental right. It may subject individuals, which has been recognized as a fundamental right. It may subject individualsto harm such asfinancial loss, loss ofreputation, and profiling[3].

Currently, India does not have a stand alone law on data protection. The usage of personal data is regulated under the Information Technology (IT) Act, 2000 is the law which regulates the usage of personal data in India. It can be clearly observed that this statutory frame work is neither adequatenor effective to ensure the protection of personal data.

In 2017, the Central government constituted a Committee of Experts on Data Protection chaired by Justice B.N. Srikrishna to examine issues relating to data protection in the country.The Committee submitted its report in July 2018 along with recommendations that led to the enactment of the Personal Data Protection Bill, 2019. This Bill was later referred to a Joint Parliamentary Committee which submitted its report in December 2021 and consequently inAugust 2022, the Bill was withdrawn from Parliament.

---

2 Sec2(13)ofDigitalPersonalDataProtectionBill,2022-"personaldata"meansanydataaboutanindividualwhoisidentifiablebyorinrelationtosuchdata.

3 "Protection of personal data and privacy" COUNCIL OF EUROPE,Available at:https://www.coe.int/en/web/portal/personal-data-protection-and-privacy#:~:text=Personal%20Data%20Protection%20Convention,known%20as%20%E2%80%9CConvention%20108%E2%80%9D.lastupdated2ndFeb2023.

Subsequently, on November 2022, the Ministry of Electronics released the draft Digital Personal Data Protection Bill, 2022 for publicfeedback.

## India's Data Protection Regime

To embark upon, the evolution of data Protection safeguard in India can be seen through various committee reports, national and international case law decisions, and foreign laws. In Ireland in the year 2014, Digital Rights, a digital rights advocacy group brought an action before the High Court of Ireland where it challenged the legality of national legislative and administrative measures concerning the retention of data relating to electronic communications by Internet Service Providers in Digital Rights Ireland v. Ireland[4], against a directive adopted by European Parliament and the Council of European Union (EU) which can be used to fight serious crimes in European Union. According to the Court of Justice of the European Union (CJEU), the directive interfered with the right to respect private life under Article 7 and the right to the protection of personal data under Article 8 of the Charter of Fundamental Rights of the European Union. Under Article 52(1) of the Charter, limitations of such rights can only be justified when they are respectful of the essence of the rights protected by the Charter, and proportionate to the legitimate aim pursued. The Court held that the directive was found to be invalid[5]. This decision was being referred to in Justice K.S Puttaswamy (Retd) v. Union of India[6] cases I and II.

The Supreme Court's Puttaswamy[7] judgments, in the year 2017 and in 2019[8] recognized the right to privacy as a fundamental right of Indian citizens and tasked the government with enacting a data protection law. Moreover, Justice Chandrachud held that information control empowers

4 C-293/12 and C-594/12

5 Digital Rights Ireland Ltd v. Ireland C-293/12 and C-594/12

6 (2017) 10 SCC 1

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

8 (2019)1 SCC 1

individuals to use" privacy as a shield" to retain control over personal information. The Court also noted that encroachment or restriction of privacy can only be allowed if the restriction satisfies the three-fold tests:

- **Legality:** There must exist a valid law allowing the restriction of privacy
- **Legitimacy:** There must be a legislated state aim justifying the restriction
- **Proportionality:** The restriction must be proportionate to the object and needs of the law. To be lucid, these tests mean that first, there must exist a valid law to justify an encroachment on privacy; second there must be a legitimate state aim to justify such a restriction and third the restriction must be proportionate to the object and needs of the law. By outlining the conditions under which the State may intervene or infringe upon an individual's right to privacy, the Supreme Court prescribed certain limitations on the State, which ultimately advanced the protection of data and informational privacy. However, the Data Protection Bill, 2022 appears to have completely forgotten and worse ignored the Puttaswamy judgment.

Moreover, in 2018 the Committee of Experts on a Data Protection Framework for India chaired by Justice B. N. Srikrishna submitted its report. The Committee observed that the regulatory framework has to balance the interests of the individual with regard to his personal data and the interests of the entity such as a service provider who has access to this data.[9] It noted that the relationship between the individual and the service provider must be viewed as a fiduciary relationship.

Besides, the committee also suggested that to prevent abuse of power by service providers, the law should establish their basic obligations, including: (i) the obligation to process data fairly and reasonably, and (ii)

9 A Free and Fair Digital Economy, PRS LEGISLATIVE RESEARCH, https://prsindia.org/policy/report-summaries/free-and-fair-digital-economy (Last visited at 10TH April 2023)

the obligation to give notice to the individual at the time of collecting data to various points in the interim.

Apart from that the Committee highlighted that consent must be treated as a pre-condition for processing personal data. Such consent should be informed or meaningful. Further, for certain vulnerable groups, such as children, and for sensitive personal data, a data protection law must sufficiently protect their interests while considering their vulnerability, and exposure to risks online. The Committee also reported that it is not possible to obtain the consent of the individual in all circumstances. Therefore, separate grounds may be established for processing data without consent. The Committee identified four bases for non-consensual processing:

(i) where processing is relevant for the state to discharge its welfare functions,

(ii) to comply with the law or with court orders in India,

(iii) when necessitated by the requirement to act promptly (to save a life, for instance), and

(iv) in employment contracts, in limited situations (such, as where giving the consent requires an unreasonable effort for the employer).

## Key Features of the Digital Personal Data Protection Bill, 2022

The Digital Personal Data Protection Bill, of 2022 gives the definition of Personal Data as "Data about an individual who is identifiable by or in relation to such data[10]". It includes directly identifiable information such as name, and contact information, as well as indirectly identifiable information such as vehicle numbers, location data, employee codes, or similar information. All these data amounts to personal data that helps in identifying an individual.

Besides, in the new Bill, Data Principal refers to the individual whose 'data is being collected'. In the case of children (<18 years), their parents/

10 Sec 2(13), Digital Personal Data Protection Bill, 2022.

lawful guardians will be considered their "Data Principals"[11]. Data Fiduciary is the entity (individual, company, firm, state, etc.), which decides the "purpose and means of the processing of an individual's personal data"[12].

The term Processing means "the entire cycle of operations that can be carried out in respect of personal data"[13]. The Significant Data Fiduciaries are those who deal with a high volume of personal data. The Central government will define who is designated under this category based on a number of factors. Such entities will have to appoint a 'Data protection officer' and an independent Data Auditor. The Bill will apply to the processing of digital personal data within India where such data is:

a) collected online, or

b) collected offline and is digitized. It will also apply to the processing of personal data outside India if it is for offering goods or services or profiling individuals in India.[14]

In addition to that, Consent is the next important aspect of this Bill. Personal data may be processed only for a lawful purpose for which an individual has given consent. A notice must be given before seeking consent. Notice should contain details about the personal data to be collected and the purpose of processing.[15]

Consent may be withdrawn at any point in time. Consent will be deemed given where processing is necessary for a) performance of any function under a law, b) provision of service or benefit by the State, c) medical emergency, d) employment purposes, and e) specified public interest purposes such as national security, fraud prevention, and information security.

Obligations of data fiduciaries are another feature of the Bill. The entity determining the purpose and means of processing called the data fiduciary

11 Sec 2(6), Digital Personal Data Protection Bill, 2022

12 Sec 2(5), Digital Personal Data Protection Bill, 2022.

13 Sec 2(16), Digital Personal Data Protection Bill, 2022

14 Sec 4, Digital Personal Data Protection Bill, 2022

15 Sec 7, Digital Personal Data Protection Bill, 2022

must make reasonable efforts to ensure the accuracy and completeness of data. It also emphasizes building reasonable security safeguards to prevent a data breach and inform the Data Protection Board of India and affected persons in the event of a breach and also recommends to cease to retain personal data as soon as the purpose has been met and retention is not necessary for legal or business purposes (storage limitation). The storage limitation requirement will not apply in case of processing by government entities.[16]

The central government may notify countries where a data fiduciary may transfer personal data outside India. Transfers will be subject to prescribed terms and conditions.

While discussing the provisions of the Bill we can clearly see that there are exemptions provided in the statute. The rights of the data principal and obligations of data fiduciaries (except data security) will not apply in specified cases including prevention and investigation of offences, and enforcement of legal rights or claims. The central government may, by notification, exempt certain activities from the application of provisions of the Bill. These include (i) processing by government entities in the interest of the security of the state and public order, and (ii) research, archiving, or statistical purposes.[17]

16 Sec 15, Digital Personal Data Protection Bill, 2022

17 Sec 18, Digital Personal Data Protection Bill, 2022

## The Main Principles of the Digital Personal Data Protection Bill, 2022

a. The usage of personal data by organizations must be done in a manner that is lawful, fair to the individuals concerned, and transparent to individuals.
b. Personal data must only be used for the purposes for which it was collected.
c. Data minimization is another principle.
d. Puts emphasis on Data accuracy when it comes to collection.
e. Personal data that is collected cannot be "stored perpetually by default" and storage should be limited to a fixed duration.
f. There should be reasonable safeguards to ensure there is "no unauthorized collection or processing of personal data".
g. "The person who decides the purpose and means of the processing of personal data should be accountable for such processing".

The Personal Data Protection Bill of 2022 also provides with various rights and Duties for Data Principals.[18] They are

a. Right to information about personal data.
b. Right to give consent.
c. Right to correction and erasure of personal data.
d. Right of grievance redressal.
e. Right to nominate.

The Data Principal are also provided with certain duties.[19] They may

a. comply with all applicable provisions of the Act.
b. not register a false or frivolous grievance or complaint with a data fiduciary or the Board.

18 §§ 12 - 15, Digital Personal Data Protection Bill, 2022

19 Sec 16 Digital Personal Data Protection Bill, 2022

c. not furnish false particulars or suppress material information

d. furnish information which is only verifiably authentic.

## Key Issues and Challenges

There are certain issues and challenges that can be pointed out in the proposed Digital Personal Data Protection Bill, 2022, they are

- Exemptions to the State may have adverse implications for privacy: Personal data processing by the State has been given several exemptions under the Bill on the basis of the security of the State, friendly relations with foreign States, maintenance of public order etc.
- The Bill may enable unchecked data processing by the State, which may violate the right to privacy: The Bill empowers the central government to exempt processing by government agencies from any or all provisions, in the interest of aims such as the security of the state and maintenance of public order. None of the rights of data principals and obligations of data fiduciaries (except data security) will apply in certain cases such as processing for prevention, investigation, and prosecution of offences.

  The Bill does not require government agencies to delete personal data, after the purpose for processing has been met. Using the above exemptions, on the ground of national security, a government agency may collect data about citizens to create a 360-degree profile for surveillance. It may utilize data retained by various government agencies for this purpose. This raises the question whether these exemptions will meet the proportionality test.
- Consent requirement should not apply where government agencies provide commercial services: The Bill provides that consent will be deemed to have been obtained for processing of data to provide benefits and services by the State and its instrumentalities. Consent requirement provides individuals control over the extent of data

collection and processing. Government and public sector utilities owned by it provide various services to individuals such as health, banking, telecom, and electricity. Thus, government health departments and companies such as SBI, BSNL, need not take consent from individuals for processing their data.

- The Bill accords differential treatment towards public and private entities performing the same function: A government company can process the personal data of its customers without obtaining their consent, and it may retain the data for an unlimited period. However, its competitors in the private sector would have to comply with these requirements. This may violate the right to equality protected under Article 14 of the Constitution.
- Bill may not ensure the independence of the Data Protection Board of India: The Bill requires the central government to set up the Data Protection Board of India. It provides that the Board will function as an independent body. The composition, terms of appointment, and manner of removal of the members will be prescribed by the central government.[20]
- Right to data portability and the right to be forgotten are not provided: The Bill does not provide for the right to data portability and the right to be forgotten. General Data Protection Regulation (GDPR) of the European Union recognizes these rights. The Srikrishna Committee (2018) also observed that a strong set of rights of data principals is an essential component of a data protection law. These rights are based on principles of autonomy, transparency, and accountability to give individuals control over their data.[21]

A. Right to data portability: The right to data portability allows data

20 Sec 19, Digital Personal Data Protection Bill, 2022

21 Alafaa, Princess, Data Privacy and Data Protection: The Right of User's and the Responsibility of Companies in the Digital World. (January 7, 2022). Available at SSRN: https://ssrn.com/abstract=4005750 or http://dx.doi.org/10.2139/ssrn.4005750

principals to obtain and transfer their data from data fiduciary for their own use, in a structured, commonly used, and machine-readable format. It gives the data principal greater control over their data and can facilitate the migration of data from one data fiduciary to another.

B. Right to be forgotten: The right to be forgotten refers to the right of individuals to limit the disclosure of personal data on the internet. Exercise of this right may interfere with someone else's right to free speech and expression and the right to receive information.

## Findings

The Data Protection Bill, 2022 is an unfortunate departure from the ethos of the Puttaswamy judgment, and other advancements made in Indian jurisprudence, which have been instrumental in centering the focus on individual rights in the discourse around privacy.

Furthermore, an idea of tribunalisation that India's legal journey must move away from. To be lucid, it introduces a Data Protection Board and then goes on to provide it exclusive jurisdiction over all disputes arising out of the provisions of the Bill. In doing so, it also explicitly excludes the jurisdiction of civil courts. It doesn't have an appellate authority over it.

Moreover, the Data Protection Bill, of 2022, which must provide primacy to individual rights, actually undermines it in favour of the interests of data fiduciaries. This is most clearly reflected in Clause 8, or the "deemed consent" clause, where the interests of data fiduciaries in processing data for a reasonable and fair purpose may outweigh any adverse effect on the rights of the data principal.

## Conclusion

In this digitalized world, bringing in legislation on data protection in the country would protect individual privacy, ensure autonomy, and allow data flow for a growing data ecosystem. It can create a free and fair digital economy where freedom is the enhancement of individual autonomy with

regard to personal data and fairness is the regulatory framework where this individual right is respected. However, it is undeniable that the proposed law has many flaws and gaps flagged by the experts. In long run, we can address the true efficiency and impact of this legislation in a country like India, where a comprehensive law that protects information security and privacy is in demand by its stakeholders.

# Cyber forensics: a techno-Legal paradigm

***Dr. Sumayya H.***[1]

Cyber Forensics is a domain in the investigation of Cyber Crimes. The focus of Cyber Forensics is to findout digital evidence and examines such evidence required to establish whether or not crime has been committed. The growth in the number of internet usage fueledby easier availability of Information and Communication Technology, the wide spread usageof mobiles and tablets, the tech-savvy younger generation, updated versions of software applications and business process outsourcing where India is a global hub of Information Technology industry are the major factors that accelerated cybercrimes. Hence there is a needto develop a best practices of data security and strong cyber forensics to control or investigatecybercrimes. Moreover, there isa needto developan irrebuttable piece of evidence and its admissibility in imparting justice.

## Relevance of the study

The analysis of de novo procedures of cyber forensics is primarily concerned with systematic identification, acquisition, preservation and analysis of digital evidence without losing itsprobative value.

The use of digital forensic evidence, its tools and purpose,

1 Guest Faculty, School of Indian Legal Thought, Mahatma Gandhi University, Kottayam, Kerala, India

The legal framework of digital evidence documentation as Forensic Life Cycle and Chain ofCustody which are the legal barriers in our system.

The parameters of admissibility digital forensic evidence and its legal bandwidth in trial andpre-trialprocedures are the corearea of the review.

## Meaning of the term Cyber Forensics

"Forensics" means belonging to court of justice. The term "Cyber" means characteristics of data relating to or involving, computers or computer networks or any electronic device which are embedded with hardware and software partsof acomputer. Cyber Forensics means characteristic of evidence that satisfies its suitability for admission as fact and fact in issue which are relevant to be admissible based on proof in the court of law.Asin the context of paper evidence, the process is clear and intuitively obvious digital evidence by its verymature is invisible to the eye. Therefore, the evidence must be developed by using tools otherthan human eye. Digital evidence is much easier to manipulate. Perfect digital copies can bemade without harming original. So, there is high risk tampering or alteration of evidenceduring the pre-trial as well as trial processes.

## Roleof Digital Forensics

Uncover and document evidence.

Corroborate evidence discovered on other ways (e-discovery)

Assist in showing a pattern of events (Data mining has application here which is done withthe help of scientifically developed tool)

Connectattackerandvictim. (Locard'sexchangeprinciple[2]).

End –to-end path, the events leading to attempt, preparation and unlawful act successful ornot2[3].

Extract data that may be hidden deleted or otherwise not directly

2 Everyoneleavesatrace

3 Same application of legal provisions in criminal law with regard to inchoateoffences.

available[4]. (This application is also done through scientifically developed cyber tools).

The key aspects of forensic data collection are:

- The tools you use to collect the data
- The techniques you use to collect and preserve the data
- The tools you use to analyse the data
- The techniques you use to analyse the data

## Legal issues needed to be proven in Acquisition of Digital Evidence

Acquisition of digital evidence is both a legal and technical problem. In fact, there two aspects are irrevocably related. The law specifies what can be seized? and what condition? From whom? from where? It requires to determine what piece of digital evidence is requiredfor examination i.e., it is a particular file, word processing document or an executableprogram. It also requires examination to determine where a particulars piece of evidence is physically located.[5] Is the file on a harddrive or Is it on a server located in other jurisdiction. I fit is so then a technical basisfor obtaining the legal authority to search.[6]

## Denovo procedures in Cyber Forensics

The denovo procedures of Forensic Life Cycle and Chain of Custody which are prerequisite in pre-trial processes ensures the admissibility of digital evidence before the court. The Cyber Forensic experts are entrusted with the responsibility of vigilant and active in all the steps of Forensic Life Cycle as well as Chain of Custody. Cyber Forensic experts are the qualified Cyber experts appointed for the specific purpose by the investigating authority from government as well as private entities.

4 Nina Godbole, Sunil Belapur, Cyber Security, Wiley Publishers, 2023, p.321

5 Id p.329

6 Ibid

Digital forensic is an application of analysis techniques to the reliable and unbiased collection, analysis, interpretation and presentation of digital evidence. Computer Forensic is the collection of techniques and tools used to find evidence in a computer. Digital forensics is the use of scientifically deceived and proven methods towards the preservation, collection, validation, identification, analysis, interpretation documentation and presentation of digital evidence derived from digital sources for the purpose of facilitation or furthering there construction of events developed by the accused or helping to anticipate unauthorized actions shown to be disruptive to planned operation[7].

## Challenges in in dial legal system

For the convenience of study, we can divide the challenges of cyber forensic as pre-trial challenges and trial challenges. The pre-trial challenge involves the cyber forensic investigation which involves two main uncompromised tasks of Cyber Forensic Life Cycle as well as Chain of Custody. The trial processes involve the admissibility of digital forensic evidence as well as its probative value.

## Cyber Forensic Life Cycle

### *1. Collection of evidence*

There are two major risks in collection of data i.e.; loss or alteration of data

It covers the recognition of incidents and its identification. For the purpose of collection some technologically developed tools are used. All these are done by an authorised officer with orwithout search warrant and complying all procedures of search in Criminal Procedure Code.The important requirement of cyber forensic tool for collection of evidence are

They must not alter the data as a side effect of the collection processThey must collect all of the data we want, and only the data we want.

7 Nina Godbole, Sunil Belapure, Cyber Security, Wiley Publishers, 2023, p.319

We must be able to establish that they worked properly, e.g., as advertised.

They must be accepted, generally, by the computer forensic investigative community. The results they produce must be repeatable.

***Tools for Collection of Cyber Forensic Data.***

1. X -ways Forensics is a software used in windows, 32 Bit/64 Bit with very detailed filtering options and is highly efficient and cheaper. This tool helps the cyber forensic experts forrecovery of evidence from digital camaras, deleted files and corrupted files.
2. Sleuth Kitused for analysing disk images and in-depth analysis offile system and recovery offile as well as used for Cyber Autopsy.
3. SANS Investigative Forensic Tool Kit (SIFT) is a multipurpose, open-source low, cost embedded tool kit which contains necessary tools for investigation. It prevents the conversionof examined evidence into read only file.
4. Encase is multipurpose tool togather data from various devices without altering the same. It supports encryption which made the data secured. After data analysis it produce a report which can be used in a court of law.
5. Computer Aided Investigative Environment (CAINE) used for investigation and can be used in recovery of damaged files, virus embedded system and deleted files.
6. Forensic Tool Kit (FTK)is used to examine various information from decrypted as well as encrypted information and information formation deleted mails[8].

8 Shubham Maheshwari, A new dimension to compact Cyber Crime, ACCLAIMS, Vol5, 2021, ISSN 25815504

## Technique for collection of Cyber Forensic Evidence[9]

### *a. Proceed and physically appear to the scene of occurrence*

The authorised Cyber Forensic official physically proceed to theplace of occurrence of alleged virtual offence scene.The official identifies or recognizes the incident. The official identifies the purpose of investigation and also arrange the resources required for investigation

### *b. Clear everyone near to the computer*

Examine the network and modem connections and check any other connections which is attached to the alleged system. If the mode misconnected with the computer the unplug it and never turn off the computer or modem or donot make a dialup because there might be a chance of rebuttal of such evidence before the court.

### *c. Carefully observe the screen display.*

If your observation of the screen display indicatesthat there is a currently running remote session, it is probably even more important the you cut the connection at once. If you can do so, it is a good idea to redirect lists to a floppy disk and never display it. By not displaying, you won't write to the hard drive whenthe DIR command completes. Instead, by redirecting to the floppy, you'll capture on safe media and, when the command closes, the residue will be written to the slack space on the floppy.Labelthe floppy and write-protect it.

### *d. Document the connections to the PC*

Document by sketching or taking a Polaroid snapshot. Then take labels and label all connections and reassemble the system exactly as same that of time of occurrence. Lastly, the controversial step: turning off the computer[10].

---

9 Peter Stevenson, A handbook for Investigating Computer Related Crime, CRC Press, Washington London, 2005, p.121to127.

10 Ibid.

## Tool Kit Used by the Cyber Forensic Expert for Collection of Digital evidence

Tools are varying depend upon on the size of disk.

- Shutdown the computer.
- Reboot to DOS (NEVER Windows) from a floppy.
- Make two physical backups of the hard drive.
- Use one physical backup to create a mirror of the machine under test; save the other forevidence.
- Analyse the mirror machine.

## 2. Search and Seizure of the Evidence

After recognition of evidence, the hard ware or the software required for the investigationshall be seized are to be seized. It includes seizure of hard drive or seizure of particular software's or relevant data in drives only. The expert shall seize only the data required for investigation Programmes if it is required.

## 3. Preservation of Digital Evidence

It involves collection and preservation in CD, USB' setcor in a protected system, where only limited forensic officials are only accessed with such devicein order to preserve data in a secure and to protect the integrity of data. Moreover, hash encryption is also used for avoid tampering of digital evidence. The most common method used for encryption during thepreservation of digital evidence is the hash encryption which allows a security measure of alteration of digital evidence collected. The task of the expert is to isolate and preserve theevidence without losing its probative value.

## 4. Examination

Examination covers duplicate and recover data. Sometimes data are present, deleted, hidden, encrypted. For the purpose of digital evidence

examination imaging of electronic media isrelevant to identify where the evidence is located. The process of creating exact duplicate ofthe original evidentiary media is often called Imaging.The Cyber Forensic Expert used certain tools for recovery of such data . They are Tools for Examination

a) FILE CARVING- file carving which is the process of recovering files without the knowledge of file structure.
b) RAID-Redundant Array of Independent (inexpensive) Disk. It gives information on location of data on different file. It is a software on which data are arrayed on different disks
c) COFEE-Computer Online Forensic Extractor-decrypt password, display all internet activity, uncover all data stored in acomputer.

## 5. Analysis

The Cyber Forensic experts analyse the type of evidence stored in the seized data. For this purpose, they have used analysis tools The expert made dead analysis and live analysis Deadanalysis is the traditional analysis of hard disk or information at rest and live analysis is the analysis of live systems or particular programmes which is running on alleged incident. The reason is that many current attacks against computer systems leave not race on the computer's harddrive, the attacker only exploit informationin the computer's memory. Another reason is in case of encrypted data, the only copy of keys to decrypt the storage inthe computer's memory. When we turn off the computer will cause the losing of information. So,the live analysis is relevantin current scenario[11].

Another analysis is the deleted file recovery with the help of tools. The stochastic forensics, another form of analysis used to identify the theft of insider data. The Steganography is the latest analysis tool used to encrypt the message in a hidden form which is often go unnoticed[12]

11 Nina Godbole, Sunil Belapur, Cyber Security, Wiley Publishers, 2023,p.346.

12 Shubham Maheshwari, A new dimension to compact Cyber Crime, ACCLAIMS, Vol5, 2021, ISSN25815504

Additionally, the assistance of telephone companies and Internet service providers (ISPs)that might require a warrant. This means that law enforcement will need to get involved, needtogetsupport from intervening system aswellas routersorWi-Fi providers[13].

The expert determines the significance, reconstructs the fragments of data and draw conclusions.

## 6. Reporting

An expert report is generated after analysis of finished. The report is presented by the expert before the variety of audience such as law enforcement officials, technical experts, legal experts and corporate management. The presentation of evidence and its analysis, interpretation and its attribution have many challenges. The following are the broad elementsof report.

1. Identity of the reporting agency.
2. Case identifier or submission number.
3. Case Investigator.
4. Identity of the submitter.
5. Date of receipt.
6. Date of Report.
7. Descriptive list of items submitted for examination, including serial number, make and model
8. Identity and signature of the examiner.
9. Brief description of the steps taken during examination such as string searches, graphic image searches and recovering erased files.
10. Results and conclusions[14].

13 Peter Stevenson, A handbook for Investigating Computer Related Crime, CRC Press, Washington London, 2005 Id p.135.

14 Nina Godbole, Sunil Belapur, Cyber Security, Wiley Publishers, 2023, p.352.

## 7. Testifying

This phase is the presentation and cross examination of expert witnesses. Only expert witnesscan address issues based on scientific, technical or another specialized knowledge. The expert testimony is based on sufficient facts or data, testimony is based on sufficient principles and methods and the expert has applied the principles and methods reliably to the facts of the case.

## 8. Chain of Custody

Chronological written record of those individuals who have has the custody of evidence fromits initial acquisition to its final disposition. The chain of custody is relevant only in trial stageeven thoughit is aprocedure as partof trial and per-trial procedures.

***Purpose of chain of custody***

It is the proponent of a piece of evidence must demonstrate that it is what it purports to be. Relevant in trial for admissibility of forensic evidence

It assumes continuous accountability. The accountability is important because, if it is not properly maintained, the evidence may be in admissible before the court.

***Chronological Arrangement of Chain of Custody***

1. Name or the initials of individual collecting the evidence.
2. Each person or entity subsequently having custody of it.
3. Dtesonwhichevidenceitemwerecollectedortransferred.
4. Deparment, agency or team name and case number where the investigation is done.
5. Brief description of the its seized.
6. Authority on which such items kept, preserved, transported with specific date andcustodian[15]

15 Id p. 357.

## 9. The Challenge of Cyber Forensics Evidence in Trial

The Court need to know where the offender and the victim came into contact with one with one another in the perpetration of the offence so that the adjudicator or the judge or Magistrate may not understand the digital tool very well. Overlooking some of the technologies utilised in investigation, misunderstanding some jargons used while prosecuting and passing judgements on such incidents without proper understanding may lead to in conclusive results, wrong interpretations etc and mistakenly erroneous acquittal or erroneous conviction of the culprits[16].

The digital evidence is admissible, authentic, complete, reliable and understandable lead the court to arrive a conclusive decision. The contents of documents and electronic evidence areproved with the report of a cyber forensic examiner called as expert witness report. The Report shall corroborate with other evidence and the Chain of custody is relevant.

## 10. Legal Provision on Cyber Forensic Evidence

INDIAN EVIDENCE ACT AND ADMISSIBILITY OF CYBER FORENSIC EVIDENCE section 65A provides that contents of electronic records could also be admitted as evidence ifthe standards provided in Section 65B is complied with. Section 65B provides that shall be considered documents, thereby making it primary evidence, if the pc which produced the record had been regularly in use, the knowledge fed into the computer was a part of the regular use of the PC and the PC had been operating properly. It further provides that each one computer output shall be considered as being produced by the pc itself, whether it hadbeen produced directly or indirectly, whether with human intervention or without. This provision does away with the concept of computer evidence being hearsay. Thus, withthe amendments introduced into the statute, electronic evidence in India is not any longer either secondary.

16 Virginiah Sekgwathe, Mohammed Talib, Cyber Security Incidents and Response, International Journal Computer Architecture and their applications, ISSN2220-9085.

- Sec 22-Oral evidence on contents of a document shall be proved on examination of person documented it and is relevant only when it is contested with regard toits genuine
- Sec 45 A –Opinion of digital examiner is relevant with regard any information in electronic form.
- SEC79AOF Information Technology Act.2000-Directs the examiner of digital evidence to provide expert opinion before any court of law.

JagjithSinghv.State of Haryana[17] that the Speaker of the Legislative Assembly of the State of Haryana disqualified a member on the ground of defection. The Supreme Court, whilst hearing the matter, also considered the appreciation of digital evidence within the sortof transcripts of digital media including the News Channels. The channels involved were Zee News channel, the Aaj Tak television channel, and the Haryana News of Punjab Todaytelevision channel. The court indicated the extent of the relevant digital materials and determined that the electronic evidence placed on the record was admissible, and upheld thereliance placed by the Speaker on the interview recorded on the CDs for reaching the conclusion that the persons recorded on the CDs were equivalent as those taking action andtheir voices were also identical. This judgment enhanced the role of Digital Evidence in perspectives of Best Evidence Rule also.

In India after the enactment of Information Technology Act, 2000 subject to satisfaction of the provisions laid down undersection 65B and ratio decidendi stipulated in Anwar P.V. v. P.K.Basheer[18], amendments in the Indian Evidence Act, 1872 and the Indian Penal Code,1860, electronic evidence is admissible.

## 11. Best Evidence Rule

The Best Evidence Rule is the cardinal principle of Evidence Act. The rule is that the best evidence is the original evidence. If the original is destroyed the copy will be accepted.

17 WP (Civil) 287 of 2004.

18 AIR 2005 SC 180.

However, the copy must be proved by awitness who can testify the contents and confirm that it is the accurate copy of the original. The Cyber Forensic expert report shall satisfy the forensic life cycle and chain of custody which made the report produced before the court as authentic and admissible even though he is producing the exact Image or Copy of alleged information or data.

## 12. Loss of Evidential Value

In trial we need reliable chain of custody software supported byexperts.

The senior experts only are accessed the data and officials are limited fromaccessingthedata. In trialstage evidence lost its value when the chain of custody was violated.

Attorneys can easily prove this because of full proof software to reveal the chain of custody.

## 13. Conclusion

It can be especially confusing to think about digital proof because, both in our currentdiscussions and in early cases, legal analysts have tended to treat "computer evidence" as if it were its own separate, overarching evidentiary category. Ofcourse, insome very practical ways electronic evidence is unique: it can be created, altered, stored, copied, and moved with unprecedented ease, which creates both problems and opportunities for advocates. But in many important respects, "computer evidence," like any other, must pass a variety of traditional admissibility tests[19].

Specifically,somecommentaryisnotveryclear whether admitting computer recordsrequires a 'best evidence' analysis, an authentication process, a hearsay examination, or all ofthe above. Advocates and courts have sometimes mixed, matched, and lumped these ideastogether by talking simply about the 'reliability' or 'trustworthiness' of computer evidence ingeneral, sweeping terms, rather than asking critically whether the evidence was 'trustworthy'inall required aspects[20].

19 IDP.153.

20 Ibid.

In India, all electronic records are now considered to be documents, thus making themprimary evidence. At an equivalent time a blanket rule against hearsay has been created inrespect of computer output. These two changes within the stance of the law have createdparadigm shifts within the admissibility and relevancy of electronic evidence, albeit certainprecautions still being necessary. However, technology has itself provided answers toproblems raised by it, and computer forensics make sure that manipulations in electronic evidence show up clearly within the record. Human beings now only got to make sure thatelectronic evidence being admitted has relevancy to the very fact in issue and is in accordance with the Constitution and other laws of the land.

# E-Commerce and its Impact on International Trade: Challenges & Way Forward

***A Lakshmi & Bini P. B.***

## Abstract

*The advancement in science and technology has simplified international trade. Business entities today use internet for a wide range of activities, predominantly referred to as E- Commerce. The WTO member countries adopted the 'Declaration on Global Electronic Commerce' in 1998 realizing the growth of e-commerce and the new opportunities for international trade. E-commerce will soon replace the traditional modes of conduct of business. A number of issues pop-up when it comes to national policy making in this field like jurisdictional issues, infrastructural bottlenecks, inadequate legal frame work, cyber security issues, trademark security problems, copyright protection issues, etc. In addition to that there are some issues relating to trust that include privacy, security, consumer protection and content regulation. As of now there are no specific legislations governing e-commerce in India. There is an urgent need for government to intervene and come up with laws. Through this paper, the researchers aim at pointing out the existing lacunae in e-commerce in connection with international trade and also make suggestions to overcome the same.*

## Understanding E- Commerce

The internet is one of the best things that has happened in the last decade. It has made possible at low-cost, individual communication from any place in the world to any other place. The appearance of the internet

among communities has brought many benefits for businesses. The internet inherently provides businesses with cost-effective means of distributing as well as obtaining information quickly. Electronic commerce (E-Commerce) is a paradigm shift and a competitive tool for small and medium-sized firms (SMFs) to conduct their businesses via computer networks including the internet. The advancement of technology has improved international business. Millions of people around the globe use the internet for everything from research to online shopping. The internet is largely affecting almost all businesses.

The various uses of the Internet by business entities include the ability to advertise, generate, or otherwise perform regular business functions. As a result, many businesses are adopting the internet for many of their operations. One effect of e-commerce is to intensify competition and produce benefits to consumers at cheaper prices and more options.[1] The United Nations Commission on International Trade Law (UNCITRAL) recognized the need for a "model law facilitating the use of electronic commerce that is acceptable to states with different legal, social and economic systems, could contribute significantly to the developments of harmonious international economic relations. Increasing number of transactions in international trade is carried out by means of communication, commonly referred to as electronic commerce, which involve the use of alternatives to paper-based methods of communication and storage of information."[2]

E-commerce is the use of the Internet to conduct national or international business transactions. E-commerce has come to play two important roles: first, as a more effective and efficient conduit and aggregator of information, and second, as a potential mechanism for the replacement of many economic activities once performed within a business enterprise

1 Malkawi, B. H. E-commerce in Light of International Trade Agreements: The WTO and the United States-Jordan Free Trade Agreement. International Journal of Law and Information Technology, Vol. 15 No.2, 2007, 153-169.

2 The United Nations Commission on International Trade Law (UNCITRAL), Model Law on Electronic Commerce, 1996 (modified in 1998).

by those that can be done by outside suppliers competing to execute these activities.[3] According to World Trade Organization (WTO), Electronic Commerce is the "production, distribution, marketing, sale or delivery of goods and services by electronic means"[4]. It is also known as the paperless exchange of business information using Electronic Data Exchange, Electronic Fund Transfers, and so on. E-commerce is not only about simple transactions of data but also general commercial acts such as publicity, advertising, negotiations, contracts, and fund settlements.[5] The number of Internet users has also exceeded two billion worldwide and is growing. The influence of e- commerce stretches even further. It is used more as a trading system in which buyers and sellers can establish a genuine market price.

Electronic commerce offers important opportunities to both developing and developed countries. The development of e-commerce is likely to have both direct and indirect impacts on international trade as well as the labour markets. The use of electronic means and the internet can make the process of initiating and doing trade a lot easier, faster and less expensive. Collecting information is a costly activity when it involves acquiring information across national borders.[6] In fact, these costs can be so high that they can be considered a substantial barrier to trade. In this respect, the internet will likely promote trade much in the same way as lifting other trade barriers would. Thus, it is the volume of international trade will likely increase. The Internet is profoundly affecting almost all businesses. The various uses of the Internet by business entities include the ability to advertise, generate, or otherwise perform regular business functions. Therefore, many firms are embracing the Internet for many of their activities. One impact of e-

3 ECLAC. Electronic Commerce, International Trade and Employment: Review of the Issues. UN, Economic commission for Latin America and the Caribbean ECLAS, Washington Office, April 2002, pp 1-30.

4 'WTO Ministerial Conferences- in brief' available at https://www.wto.org.

5 Sharma, Vakul, Legal dimensions of cyberspace (Indian Law Institute, New Delhi, 2004) Page no. 51.

6 Rolf H Weber, International E- trade, The International Lawyer , FALL 2007, Vol. 41.

commerce is to intensify competition and produce benefits to consumers in lower prices and more choices.

## International Instruments Governing E-Commerce

International Trade Rules are made to avoid barriers in trade imposed by national laws. There are various tariff and non-tariff barriers restricting free trade. Since e-commerce takes place virtually, the imposition of non-tariff barriers are more common. There was a time when trade on internet remained largely unregulated. But the scenario today is a lot different. Hence, execution of e-commerce falls under the framework of WTO. WTO is mainly composed of three main agreements of GATT[7], GATS[8] and TRIPS[9]. GATS[10] applies to measures affecting trade in services. E-commerce comes into picture when from the seller and provider of services offers the products abroad or when the recipient is in another country.

One of the earliest documents that influenced the regulation of e-commerce is 'A Framework for Electronic Commerce' formulated by Clinton administration in 1997. This document stated that while self-regulation is the guiding force, regulation is necessary to develop a simple legal environment on e-commerce. It states: "In some areas, governmental interference is necessary to facilitate e-commerce and protect consumers. In such areas the government should ensure competition, protect intellectual property and privacy, prevent fraud, foster transparency, support commercial transactions and facilitate dispute resolution."[11] It was this document that

7 General Agreement on Tariff and Trade 1994 https://www.wto.org/english/docs_e/legal_e/06-gatt_e.htm

8 General Agreement on Trade in Services 1995 https://www.wto.org/english/tratop_e/serv_e/gatsqa_e.htm

9 WTO Agreement on Trade Related Aspects of Intellectual Property Rights https://www.wto.org/english/tratop_e/trips_e/trips_e.htm

10 supra 2

11 The Framework for Global Electronic Commerce https://clintonwhitehouse4.archives.gov/WH/New/Commerce/read.html

forced the international organisations like UNCITRAL[12] and ICC[13] to formulate international policy with respect to e-commerce.

Electronic Data Interchange (perform business functions automatically without any human intervention like processing of purchase order, sending of invoice to consumers, etc.) was in use right from the 1980s and continues to be in use even today. EDI has numerous advantages like lowering transaction cost, fewer errors, speedier response, etc. The United Nations Economic Commission for Europe (UNECE[14]) was the first to take up the task of standardization of EDI which resulted in the formation of UN/EDIFACT[15]. The code formulated by ICC is the Uniform Rules of Conduct for Interchange of Trade Data by Teletransmission (UNCID[16]). Many provisions in UNCITRAL can be traced to UNCID.

UNCITRAL Model Law on Electronic Commerce was adopted in 1996. A model law does not have the same legislative weight as that of a convention and also fails to bring the level of unification brought in by conventions. States are at liberty to either adopt the model law as it stands or to make their laws using the model law as a starting point. Article 5, 6, 7, 8, 11 and 12 allow states to limit application to specific areas.[17] The aim of the Model law on Electronic Commerce is to facilitate electronic commerce by eliminating the legal hurdles. The Guide to enactment of Model laws on Electronic Commerce aids interpretation. The guide states the purpose of enacting the model law on Electronic Commerce which is to facilitate e-commerce among and within nations, to validate transactions entered into by means of new information technologies, to promote and encourage

12 United Nations Commission on International Trade Law 1966 https://uncitral.un.org/

13 International Chamber of Commerce https://uncitral.un.org/

14 United Nations Economic Commission for Europe https://unece.org/

15 United Nations rules for Electronic Data Interchange for Administration, Commerce and Transport https://unece.org/trade/uncefact/

16 Uniform Rules of Conduct for Interchange of Trade Data by Teletransmission 1988 https://unece.org/trade/uncefact/part-2-uncid

17 Article 11(2) UNCITRAL

implementation of new information technologies, to promote the uniformity of law and to support commercial practice. There is no mention in the model laws on Electronic Commerce that it would apply to e-commerce transactions in the international arena. It is intended to apply to both domestic and international commercial transactions conducted electronically.

## Impact of E-Commerce on International Trade

E-commerce has brought opportunities for both the developed and developing nations. The use of electronic means and the internet has made the process of initiating and doing trade a lot easier, faster, and much cheaper. Collecting information across borders through the traditional modes is so expensive that it generally turns into a trade barrier. Finding the right supplier, specifying the product's requirements and quality, negotiating the price, arranging deliveries and marketing products are all very expensive. With the internet and e-commerce applications, a whole range of these activities can occur without having buyer and seller in close physical proximity. In this respect, the internet can help in eliminating all the prospective trade barriers. This will eventually lead to increase in volume of international trade.

With the internet, markets are more organized and have evolved as e-commerce. It has resulted in reduction of information costs and has also facilitated the interaction between consumers and sellers buying and selling goods and services electronically. This has in turn resulted in eliminating the most important barrier in traditional business, geographic proximity. E-Commerce also has a significant impact on trade in services. It has the potential benefit of reducing the cost of imports. Even if a country does not export any services, it can benefit from imports of services by paying for them in terms of goods. Cheaper availability of medical, engineering and architectural services, long-distance learning and reduced costs of transactions can confer benefits even if the country does not immediately export the services traded through Internet.

Several recent studies have asked whether internet use affects trade. For example, using data from 20 low and middle income countries in Eastern Europe and Central Asia, a research shows that enterprises with internet connections export more, as a share of their total sales, than enterprises without connections.[18] It was concluded that the use of internet is significantly correlated with trade after 1996.[19] The same research also found that internet has a greater effect on trade in developing countries than it does in developed countries.[20] In a second paper, the same researchers found that exports of services to the United States grew more quickly for countries with greater internet penetration in a sample of 31 middle and high-income countries[21].

## Challenges in E-Commerce

### *I. Inadequacy in National Legislations*

The lack of proper legal and regulatory framework in many specific areas of e-commerce is a clear indication of the main challenges of e-commerce today. Presently the laws governing e- commerce transactions are the Information Technology (IT) Act 2000, Indian Contract Act 1872, Sale of Goods Act 1930 and Competition Act 2002. Unfortunately, there is no specific legislation to guard e-commerce in India today. The weak cyber security law in India is the reason why Indian people as well as the e-commerce industries face so many challenges. They fail to enjoy a consumer friendly and business-confidant environment for e-commerce in India.

Cyber law in India tries to attend these challenges and requires compliance with IT Laws by business houses engaging in e-commerce. The

18 Clarke, G. R.G., (2001). Does Internet Connectivity Affect Export Performance? Evidence from the Transition Economies.Mimeo, World Bank, Washington DC.2001.

19 Ibid

20 Ibid

21 Daly, John and Robert R. Miller. Corporations' use of the internet in developing countries. Discussion Paper # 35, International Finance Company. Washington DC.1998.

Indian Information Technology Act, of 2000 makes it mandatory to set up corporate compliance programs including cyber law compliance program. The IT law mandates all companies to have an information technology security policy. These documents the architecture of the network, the roles and responsibilities of employees, security parameters, and authorization required for data access, among other things. Other compliances that are required include relating to the retention and authentication of electronic records and the security of data. Moreover, the Indian Information Technology Act of 2000 provides for further personal liabilities.

The IT Act provides that where a person committing a contravention of any of the provisions of this Act or of any rule, direction, or order made there under is a company, every person who, at the time the contravention was committed, was in charge of and was responsible to, the company for the conduct of the business of the company as well as the company, shall be guilty of the contravention and shall be liable to be proceeded against and punished accordingly.[22] However, the proviso to section 85 (1) provides that such a person will not be liable for punishment if he proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent such contravention. The rapid pace of growth of the commerce industry is not only indicative of the increasing receptiveness of the public but has also brought to the fore the issues that the legal system of the country has been faced with.

From the initial years when the internet was a new phenomenon to recent times where the internet has become a basic necessity for every household in most metropolitan cities, the e- commerce industry has come a long way. The legal system has constantly tried to catch up, especially with the enactment of the various rules under the IT Act to deal with a host of issues emerging from the use of the internet. Moreover, the IP issues in e-commerce transactions have taken a new form with users finding loopholes to not only easily duplicate material but also mislead other users. Hence,

22 Section 85 (1) of the IT Act.

much more is needed to effectively regulate the tangled web.[23] The growth of E-Commerce has created the need for vibrant and effective regulatory mechanisms, which would further strengthen the legal infrastructure that is crucial to the success of electronic commerce.[24] The rapid advancement of information technology poses challenges to legal systems all over the world. Transactions accomplished through electronic means collectively 'electronic commerce' have created new legal issues.

### *II. Consumer on Internet*

Traditionally we only had the Consumer Protection Act, 1986 and the Sale of Goods Act, 1930. However these domestic legislations were not sufficient to tackle the problems faced by consumers in e-commerce. These domestic legislations had territorial limitations but in e- commerce the buyer and seller may be located in any part of the world. In order to overcome these challenges, a new Consumer Protection Act was enacted in 2019. Following this was passed the Consumer Protection E-Commerce Rules 2020. Now consumers falling under B2C e- commerce also can avail protection from unfair trade practice, fraud, defective products, etc.

In e-commerce the rights and obligations of parties are generally decided based on contract entered into between the parties. And often these are in the form of standard form of contracts drafted by seller. There by making the contracts one-sided and limiting liability of the seller. Only a handful of consumers really care to read the terms of such contracts. This gives vendors the opportunity to draft the contracts, benefitting them and adversely impacting consumer interests. It is high time to regulate such unfair terms of contract. All such contracts should be reviewed by a body that ensures the rights of none of the parties are compromised. Especially the rights of weaker section, consumers' should not be affected adversely.

23 8 Mitra, A. (2013). E-commerce in India-A Review. International journal of marketing, financial services & management research, 2(2)

24 Ahmad, F. (2001). Electronic Commerce: An Indian Perspective. International Journal of Law and Information Technology, 9(2).

Considering the unequal bargaining position of consumers the OECD issues in 1998 'Guidelines for Consumer Protection in the Context of Electronic Commerce'. These recommendations include Information about Business, Information about Goods or Services and Information about Transactions.

In today's world especially post pandemic there can be seen a dramatic increase in shopping over internet. Not only is the consumer's freedom to negotiate compromised but also the market in which trading takes place fails to provide relevant information for making proper decision. Advertisements also fail to guide the customers in the right direction. There are many fraudulent schemes released to attract more and more consumers. There is a legal vacuum when it comes to regulation over these things on the internet. Further Indian court decisions are often delayed and enforcement is even more problematic. Yet another major issue is making payments online safely. In order to facilitate faster development of international commerce between businesses and between businesses and consumers, legislations have been enacted to confer legal recognition to electronic records. Section 4 of the Information Technology Act, 2000 extends legal recognition to electronic records.

### *III. Jurisdictional Dilemma*

When defendant is not the subject of the same national law as that of the plaintiff the judiciary has to step in. In e-commerce transactions these problem are sure to arise. And when defendant does not have a physical place of business in India it gets even more difficult. In order to overcome the issue of enforcement of rights of parties separated by countries and who are strangers to one another the Draft Hague Convention on Jurisdiction was prepared. The convention was intended to apply when all the parties are not habitually residents of the same country.[25]

WIPO in its Primer on Electronic Commerce and Intellectual Property Issues offers an exhaustive analysis of issues in determining jurisdiction in

25 Article 2 of Hague Convention

medium like internet that has no physical boundaries. Further the Information Technology Act, 2000 provides for application of the act to any offence or contravention committed outside India by any person.[26] The provisions of the Act will also apply to any offence or contravention committed outside India by any person irrespective of his nationality.[27] The act will also apply to offence or contravention involving a computer or computer system or computer network located in India.[28]

The issues concerning jurisdiction on transactions over internet has not received the necessary attention. It is left to the parties to determine the jurisdiction to resolve future disputes at the time of entry into the contract. When contract is entered into between two business men the chances of negotiation is more. But when it is entered into between a consumer and seller the chances of abuse of rights of consumer is high. Even more important than that, is to ensure a mechanism for enforcement which would be equitable to both the parties, especially consumers. Until all the countries unanimously agree to sign a convention, a mechanism needs to be found to enforce the judgments of one country over another country.

### *IV. IPR Related Problems*

There are a number of intellectual property rights that exist in any website. Any logo or branding is likely to be protected by registered trademark rights or under passing off.[29] Under the Copyright Act, parallel import is not permitted unless it is for domestic use. The terms import and importer have not been defined in the Copyright Act but Courts have held 'import' to mean bringing into India from outside India.[30] For instance, a book that has been published and different publishers are given rights in

26 Section 1 of IT Act, 2000

27 Section 75(1) of IT Act, 2000

28 Section 75(2) of IT Act, 2000

29 Alic, J. (1994) "Technology in the service industries" International Journal of Technology Management, 9, 1-14.

30 Gramophone Company of India Ltd. v Birendra Bhadhur Pandey, AIR 1984 SC 667.

different countries. One enterprising publisher puts the entire book online and sells it to people. Selling it to the public other than in the country where he has rights could be an infringement. The Copyright Act may allow every person in India to download one copy for domestic use. This can cause a loss to the publisher in India. Separately, the publisher who puts the book online could be hauled up for publishing outside the territory in which he has the right to publish even if the server is located in the same country.

In this digital era, access to copyrighted works becomes easier: music, videos, and books are available, just by clicking. Music, pictures, photos, software, designs, training modules, systems, etc. can all be traded through e-commerce, in which case, IP is the main component of value in the transaction. This fact increases the chance of infringement. Indeed, the selling of counterfeit product, through an e-commerce platform, constitutes a challenge for IP enforcement. Trademarks infringement causes considerable losses to the IP owner. The IP assets are mostly the substantial parts of the enterprise resources. Therefore, entrepreneurs should invest in the protection of their property. The Indian Copyright Act is unable to protect the unauthorized distribution and use of work over the internet. Infringement over the internet and piracy pose a threat to creative works worldwide and thus the growth of the internet, e-commerce, and the digital economy. As per the Indian Copyright Act, of 1957 literary works, pictures, sound recordings, and other creative works are protected from being copied without the permission of the copyright holder.[31] It is yet unclear how copyright law governs or will govern these materials as they appear on the Internet.

In electronic commerce, there are two major issues concerning trademarks: On the one hand, trademark infringement involves physical goods. On the other hand, trademark infringement in relation to transaction information. In the case of physical goods, the infringement concern is the sale of counterfeit goods via an e-commerce platform; or the sale of parallel imported products via an e-commerce site. Most of the time, we can find a

31 Section 13 & 63 of the copyright act 1957.

fake product on the internet marketplace, which can sometimes confuse customers due to its similarity to the original. Infringement of trademarks on transaction information: The domain name is the most common example. For example, a company creates a website by using another company's trademark as the domain name. Both companies may sell the same goods or engage in different activities, but the main deal is that the other company wishes to confuse the public in order to increase its business. There are issues of relevance for which the current legal framework does not provide any statutory remedies such as the punishment for the activities of intermediaries for copyright infringement, the rights management information, the protection of anti-circumvention devices, etc. The society must be educated on the necessity of Copyright protection to prevent any unauthorized use.

## Way Forward

The rapid growth of e-commerce has created the need for a vibrant and effective regulatory mechanism, which would strengthen the legal infrastructure that is crucial to the success of e-commerce in India. It has always been the allegation that the weak cyber security laws in India and the absence of a proper e-commerce regulatory framework is the reason why Indian people as well as the e-commerce industries face so many challenges in enjoying a consumer-friendly and business-confidant e-commerce environment in India. So, the government should develop a legal framework for e-commerce so that both domestic as well as international trade in India flourishes. At the same time the basic rights such as privacy, intellectual property, prevention of fraud, consumer protection etc. should be taken care of.

Legal community in India is required to be an expert in order to guide entrepreneurs, consumers and even courts in a manner that the fast emerging business module is enabled to adhere to existing legislations normally applicable to business transactions in conventional modules. Simultaneously, it should ensure that the advantages of technology are availed of unhindered by judicious evolution of law through learned interpretation of court still a

consensus emerges that a specialized law to govern and regulate certain aspects of e-commerce is imperative and an exclusive necessity. Better enforcement policy as well as rules and regulations pertaining to e-commerce sector will contribute significantly to growth of this sector in the long run.

As far as domestic e-commerce is concerned there are sufficient laws present in India except in a few jurisdictional issues when there is a shift from "in rem" to "in personam" jurisdiction such as when e-commerce involves disputes related to infringement of intellectual property rights. There is a need for enactment of statute in India based on the theories like "minimum contact" and "long arm statute" of the United States of America. Generally the contracts entered into between the buyers and sellers are one sided standard form of contract. Hence the chances of seller fooling the consumers are very high. There should be increased opportunities to read the terms of e-contract. Law should impose mandatory protective terms that are important to consumers. Vendors should also highlight problematic terms in bold. Consumers can be given the option to click 'I Agree' only next to all contentious term.

# Quelling of Personal Data and Privacy in Online Luxury

***Anagha Biju***[1]

## Abstract

*Privacy is being engaged in one's own personal space. The technological advancement made human life much easier and more luxurious, as the world is now a global village connected by people through the internet. This transition not only led to economic development but also increased consumer exposure to the world market. From new gadgets to groceries, one can purchase them online; extending this line further, a wide variety of activities can be done by people, including trading and gaining knowledge, as well as communicating with people across the world in seconds. But by being an active user of the internet and technology, one is also becoming a victim of privacy and personal data invasion. Knowingly or unknowingly, people are exposed to privacy invasions through cookies, email bugs, and so on. From the harmless IP address to the regularly used keywords, they can jointly collect the personal data of that particular user without the user's consent or without him being completely helpless over his personal records. This third-party exploitation is increasing as the law is not in pace with advanced technology. To what extent privacy and personal data can be protected is still a question, as the flow of cyberspace is global and different nations have different approaches to the protection of privacy and personal data. India, as a democratic republic, has given its people fundamental rights. Though*

1 Declaration and acknowledgment
"This research work has not been submitted elsewhere for award of any degree or for purpose of publication. The material borrowed from other sources has been duly acknowledged."

*the right to privacy is not expressly defined, through judicial interventions, it is incorporated in Article 21 of the Indian Constitution under the right to life.*

*All human beings have three lives: public, private, and secret. Gabriel García Marquez So, it is necessary to protect individuals from invasions of privacy and personal data to keep the spheres of private and public life separate.*

**Key Words:** Privacy, Personal data, Invasion, Technology, Internet, Judiciary, Fundamental rights

## Objectives

This paper aims to understand how far the right to privacy and personal data is protected in India through the Information Technology Act, 2000, and other regulations, as well as analyse different nations' regulatory models in this regard. And also to find out whether an international standard can be brought out to ensure uniformity in personal data and privacy protection all over the world.

## Introduction

A changing shift will always be welcomed with open arms. With globalisation and economic development, we reach the paramount stage where digital footprints become our luxury. Pandemics and lockdowns not only brought difficulties and economic instability, but they also marked a changing phase in which both technological advancement and a convenient global village were created. This also elevated the risk and potential threats that an individual may face through privacy violations and invasion of personal data by online platforms, as there is only a blurred line between public and private data that one shares on the internet.

As cyberspace is not barred by any fences or national territories, it is also difficult to find answers for these violations, and as we move over territories, the laws that regulate cyberspace also differ. Technologically advanced nations may have more regulatory measures than developed and developing nations. And due to this jurisdictional difference, the gravity of punishments may also differ.

India, being one of the democratic republics, has given its people the right to privacy as part and parcel of Article 21 of the Indian Constitution. And this right has been processed and defined by the judiciary many times as a part of Art 21 of the Indian Constitution.

## Internet Privacy and Data Protection

How will you feel when your information is gathered and sold in cyberspace? This is what a hacker named Tom Liner did to over 700 million LinkedIn users. And this was not reported back 10 years, this is something that happened only 2 years ago. The same happened to Wattpad readers too. A similar issue was addressed when Zuckerberg tried to link the personal details of his users between WhatsApp, Facebook, and Instagram. This all makes it difficult for internet users to understand how their privacy is actually protected and to what extent they have control over their personal data.

Privacy in a technology-driven world is a difficult proposition. There are many ways to catch a person's digital footprints if they browse the internet for various personal reasons. It all begins with the capture of the IP (Internet Protocol) address. This is a kind of personally identifiable information that is automatically captured by another computer when any communication link is made over the internet. And this results in the easy identification of the computer resource as each computer produces a unique IP address by the ISP (Internet Service Provider). Whenever a person browses, visits a site, sends an email, or chats online, he leaves his 'distinctive' address behind[2]. Through all these ways, a person's right to privacy and personal data are taken by a third party without the individual's consent.

In the judicial decision in Aadhaar case[3], the court pointed out that the right to privacy can be claimed against a state or a non-state entity in this

2 VAKUL SHARMA & SEEMA SHARMA INFORMATION TECHNOLOGY LAW AND PRACTICE 299 (6TH ed, 2019)

3 K. S. Puttuswamy v. Union of India (2017) 10 SCC 1; AIR 2017 SC 4161

digital world. The right of an individual to exercise control over his data and to be able to control his or her existence on the internet and the unauthorised use of such information may, therefore, lead to a violation of this right.[4]

As more and more economic activities are held on the internet, the importance and want for adequate legislation governing personal data and privacy are being recognised. Almost 137 of the world's nations now have their own laws to regulate cyberspace and protect individuals' personal data and privacy. The first step towards privacy protection started in 1973, when the US Department of Health, Education, and Welfare (HEW) proposed a set of codified fair information practises known as the HEW Principles. In the year 1980, a new phase for the protection of personal data in the cyberspace was marked when the Organisation for Economic Cooperation and Development (OECD) formulated eight principles based on the core principles of HEW for the Fair Information Practises codified as Protection of Privacy and Transborder Flows of Personal Data in the OECD4 Principles. The OECD has historically created internationally agreed-upon codes, practises, decisions, recommendations, and policy instruments. The eight principles of OECD[5] published in 1980 were agreed upon by member countries, including the United States, through a consensus and formal ratification process. These OECD guidelines form the basis of many modern international privacy agreements and national laws, and these eight principles from 1980 are referred to by the U.S. Government Accountability Office as key principles for privacy protection.

The next major development in data protection policies happened only in 2018. In that year, the General Data Protection Regulation (GDPR) was introduced by the European Union for the protection of personal data and the privacy of European citizens. This is regarded as the most advanced and

4 Ritansha Lakshmi, Case Summary: Justice K. S. Puttuswamy (Retd.) vs. Union of India, 2017 LAWLEX.ORG (April 10, 2020,10:10 pm),

5 1. Collection Limitation Principle 2. Data Quality Principle 3. Purpose Specification Principle 4. Use Limitation Principle 5. Security Safeguards Principle 6. Openness Principle 7. Individual Participation Principle

well-grounded legal legislation for the protection of personal data and privacy and its ongoing security. The effect of GDPR created a drastic shift in how data protection and privacy were viewed by individuals, organisations, and countries and saw a rapid global trend in the same direction. Under GDPR, the data is classified into two types[6] having eight core principles.[7]

## Constitution and Right to Privacy

Privacy can be described as the 'right to be left alone'. And the right to privacy can be described as the right of a person to enjoy his own presence and decide his boundaries, physical, mental, and emotional interactions with other people[8] This was originated by Warren and Brandeis in their essay "The Right to Privacy" in 1890.[9]

Though the constitution of India never guaranteed the 'right to privacy' as a fundamental right, the Supreme Court of India was always there to rescue the citizens by construing the right to privacy as a part of the "right to protection of life and personal liberty'. Keeping in view the scope of 'personal liberty', Article 21 has turned into a safeguard against arbitrary legislation.

## Legislations of Different Nations on Protection of Personal Data and Privacy

Europe: The emergency of GDPR was not only providing its citizens with localised personal data protection but more as an international law for the protection of privacy and personal data of European Union citizens that was processed by any organisation internationally. The GDPR also provides for punishments and damages. This all makes GDPR a global enforcement

6 Personal data and sensitive data.

7 1.The right to be informed, 2. The right of access, 3. The right to rectification, 4. The right to erasure, 5. The right to restrict processing, 6. The right to data portability, 7. The right to object, 8. Rights in relation to automated decision making and profiling.

8 Supra 1, at 290

9 Ibid 7

effort towards more meticulous and diligent laws and regulations regarding data protection in the future.

USA: Even though the USA doesn't have any privacy protection laws at the federal level, the country has several federal laws. As there is a dissolution of power, the state governments have created their own data protection laws. California's legislation is considered among the most forward-thinking, with the CCPA (California Consumer Privacy Act) providing robust privacy rights and consumer protection[10]. And many other Acts which deals with data protection and privacy such as The Computer Fraud and Abuse Act (CFAA), The Children Online Privacy Protection Act (COPPA), Video Privacy Protection Act, 2012(VPPA), Sarbanes-Oxley Act, 2002(Sox), Gramm-Leach Bliley Act, 2012(GLBA), Federal Fair Credit Reporting Act, 1970(FFCRA) and so on.

Canada- The government implemented the PIPED (Personal Information Protection and Electronic Documents Act) that is aligned with EU data protection law. The Act is very much consistent with global privacy policies and applies to federal works, business and every other trade and commerce when there is a collection, use or disclosure of personal information during any commercial or cross border activities. And later in 2020 the government also introduced The Digital Charter Implementation Act.

South Africa- Protection Of Personal Information Act (POPIA) was implemented by the government of South Africa in the same manner as the area is treated under GDPR.

Many other countries also implemented their own legislation for data protection and privacy for their citizens. According to data from the United Nations Conference on Trade and Development (UNCTAD), an estimated 137 out of 194 countries have put in place legislation to secure the protection of data and privacy, with Africa and Asia showing 61% (33 countries out of

10 Beyond GDPR: Data Protection Around The World, THLES (May 10, 2021,11:00 pm), https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/magazine/beyondgdpr-data-p rotection-around-wo

54) and 57% adoption respectively and only 48% of Least Developed Countries (22 out of 46) have data protection and privacy law[11].

## India and its Cyber Security Laws

While looking through the legal frameworks in India regarding privacy and data protection we can see that India is still a cusp for the introduction of data protection policies and the most distinct law concerning this subject is the Information Technology Act (ITA) 2000 and a number of rules and regulations associated thereon. Only a few sections of the Act speak about the protection of personal data and privacy such as section 43, section 66E, and section 72. This shows how much evolution had occurred over a decade on the topic of personal data and privacy.

Since 2010 the emerging need of data protection based on privacy invasion has been addressed by the DSCI (Data Security Council of India) and pointed out the need for a set of standard norms for the collection, processing and using of personal data in such a way which violates personal privacy. At present the followed rules are under the Information Technology "Reasonable security practices and procedures and sensitive personal data or information" Rules 2011[12]. The rules addressed rights to the citizens and obligations on the corporate body to protect consumer privacy. The rules also recognise sensitive personal information and put a duty on the corporation to publish their privacy policies, giving individuals the right to access and correct their information and also to obtain a consent from them for the disclosure of their sensitive information except in case of law enforcement or for the best interest of public or for violation of any law.

11 Digital Personal Data Protection Bill, 2022 [UPSC Current Affairs], BYJU'S EXAM PREP, (12 AM), https://byjus.com/free-ias-prep/digital-personal-data-protection-bill-2022/

12 Internet Privacy in India, THE CENTRE FOR INTERNET & SOCIETY (12:05 AM), https://cis-india.org/telecom/knowledge-repository-on-internet-access/internet-privacy-in-india#fn14 11 11Internet Privacy in India, THE CENTRE FOR INTERNET & SOCIETY (12:05 AM), https://cis-india.org/telecom/knowledge-repository-on-internet-access/internet-privacy-in-india#fn14

Though the rules provide the desirable data protection it was not recognised by the EU as there exist gap between these legislations in its implementation mechanism leaving a number of institutions unnoticed and unclear about its applicability by the institutions.

In 2011 the Cyber Café Rules were implemented under the ITA, 2000 which completely takes away the rights of the café users as they have to submit detail of the users, such as their name, address, contact number, gender, log in and log out time, history of the web address used as well as the proxy servers used for a period of one year. This clearly curtains the users right to privacy as well their freedom of speech and expression enumerated under the Constitution of India. Also, the greater power of law enforcing organs to interfere with consumer's online privacy under the IT Act is an example of how much power the government has on consumer data. The implementation of the Central Monitoring System by the Indian Government is another example of the Government seeking greater access to communications[13]

In the year 2012, the National Privacy Policy was formulated by an expert committee under the chairmanship of Justice A.P. Shah. Committee recommended a set of privacy policies and legislations and also listed nine National Privacy Principles that both the private and public sector data collectors must follow. These principles stand in line with other global standards like EU, OECD, APEC principles on this same subject matter.

The most noticeable step towards a legislation on personal data and internet privacy only happened when the SC held in its 2017 judgement that right to privacy is an inherent part of Article 21 under part three of Indian Constitution. The nine-bench ruling however didn't provide a definition for the term privacy but explained it in a different Indian context. The court commended that it is the responsibility of the state to protect the information privacy of the individual and give them autonomy over their personal privacy and make decisions on it. As a result of this a commission under the

13 Ibid 11

leadership of Justice B. N. Sri Krishna was formed for the formulation of a data protection regime to combat the misuse of user data by the social media networks[14] . The result of the committee was the Personal Data Protection Bill of 2019. The bill however dissolved the structure of the Data Protection Authority (DPA) and gave the central government the power to exclude any government office from its preview14.[15] Th bill also excluded the basic principle of providing protection to the user data and their privacy.

Due to the criticism faced by the bill the parliament formed a Joint Parliamentary Committee (JPC) for the further examination and giving a new tone to the bill. The JPC was chaired by P.

P. Choudhary. After several sessions the committee unanimously suggested for the expansion of focus and the ambit of the bill to cover both personal and non-personal data as it is difficult to separate their spheres. The new suggestions added strength to the bill and was forwarded to the Parliament and was implemented. However, the bill was later withdrawn citing that the provisions of the bill were inadequate to meet the global standards on data privacy.

In 2022 the old bill was again restructured and introduced as Digital Personal Data Protection Bill, 2022. The new bill introduced provisions for the setting up of a Data Protection Board (DPB) and officers on behalf of the same to adjudicate on the matters related to data protection. The principal data user was given the right to seek for erasing their data from the companies. As well as listed the matters on which the government can breach the data protection policies. The bill also provided an additional layer of protection to its citizens and was consistent with laws of the EU, Singapore and many other nations.

---

14 Khushboo Garg, Social media and Privacy: Data Protection Law, Need of the Hour? LEGAL READINGS (March 3, 2021, 11:30 am), https://legalreadings.com/social-media-and-privacy-data-protection/

15 Abhijit Ahaskar, India's Data Protection Bill: A timeline of everything so far, TEACHCIRCLE (Nov 29,2021,12:2 pm), https://www.techcircle.in/2021/11/29/india-s-data-protection-bill-a-timeline-of-everything-so-fa

## Creed and Conclusion

As we live in a fast forward world it is difficult to control the endless flow of data through cyberspace. Each nation is doing its best to protect the data privacy of its citizens. However, a common ground to deal with them together will be a difficult task as the technological development and advancement differ from nation to nation. But setting up a consortium will be a right set as it can monitor and regulate a common issue affected by a number of nations. As well as it can advance emerging countries on setting up of their own legislation consistent to the global standards. The unawareness of the people regarding these laws also make the privacy policies ineffective as the major concern of social media users of today's generation is not on the violation of their personal data but on the number of their followers and free accessibility the networking sites provide them.

India being the global hub of human resources makes this the right time for the implementation of a data protection legislation. And the current bill is in many ways up to the global standards though there are some criticisms and concerns on it, it is still a right step because a room of improvement is always good for a better vision!

## References

1) Information Technology Act,2000 Bare Act.
2) Dr. R. Myneni, Information Technology law, 2nd ed
3) Vakul Sharma and Seema Sharma Information Technology Law and Practise, 6th ed.
4) State of Privacy India, https://privacyinternational.org/state-privacy/1002/state-privacy-india
5) Social Media and Privacy: Data Protection Law, Need of the Hour? https://legalreadings.com/social-media-and-privacy-data-protection/
6) India's Data Protection Bill: A timeline of everything so far, https://www.techcircle.in/2021/11/29/india-s-data-protection-bill-a-timeline-of-everything-so-far
7) Internet Privacy in India, https://cis-india.org/telecom/knowledge-repository-on-internet-access/internet-privacy-in-india#fn14

8) The evolution of India's data privacy regime in 2021, https://iapp.org/news/a/the-evolution-of-indias-data-privacy-regime-in-2021/#:~:text=rss_feed,The%2 0evolution%20of%20India%E2%80%99s%20data%20privacy%20regime%20in%202021,-schedule

9) A look at proposed changes to India's (Personal) Data Protection Bill, https://iapp.org news/a/a-look-at-proposed-changes-to-indias-personal- data-protectionbill/#:~:text=rss_feed,A%20look%20at%20proposed%20changes%20to%20India%27s%20(Personal)%20Data%20Pr otection%20Bill,-schedule

10) India: Data Protection Laws in India - Everything You Must Know, https://www.mondaq.com/india/data-protection/655034/data-protection-laws-in-india---everything-yo u-must-know

11) Digital Data Protection Bill, 2022, https://byjus.com/free-ias-prep/digital-personal-data-protection-bill-2022/

12) Data Protection Laws and Regulations in India 2022-23, https://iapp.org/news/a/a-look-at-proposed-changes-to-indias-personal-data-protectionbill/#:~:text=rss_feed,A%20look%20at%20proposed%20changes%20to%20India%27s%20(Personal)%20Data%20Pr otection%20Bill,-schedule

13) Social media: How do other governments regulate it? https://www.bbc.com/news/technology-47135058

# Social Media Intermediaries and Obcenity

***S. Aparajitha[1] & B. Aditya Krishnan[2]***

## Abstract

*Intermediaries have the responsibility to restrict the explicit sexual contents which are posted and circulated in their own respective platforms. Each social media platform has their own community guidelines and necessary action will be taken if the subscribers tend to breach those guidelines. One of the many restrictions in those guidelines is limitation on posting and transmission of nudity or sexual contents. However, certain platforms like Twitter does not care much about restricting the sexual contents which are available to the general public. It sure does have some regulations regarding it yet it is not good enough to prevent it from reaching the eyes of minors. As a matter of fact, a certain amount of population belongs to the minors who are the contributors to this type of contents. Some Subscribers believe that the heavy traffic in profile visits which keep the subscribers hooked to their platform as the opponents are pretty strict with their guidelines regarding sexual contents is the reason for the minimal restrictions. The social media platforms might see this feature as a crowd puller. Some believe that these apps genuinely want to allow anything and everything a subscriber wants to be posted. A set of people believes that the fear of losing the subscribers might be a reason to not disturb that area as 150 million followers dropped on*

1 Sastra Deemed to be University 5th Year, B.COM, LLB (Hons) Address: No 31, Door No 1/236, 9th Cross Street, Subhashree Nagar, Extn 2, Mugalivakkam, Chennai 600125 Email ID: aparajitha.selva@gmail.com Contact Number: 7338717200

2 Sastra Deemed to be University 5th Year, B.COM, LLB (Hons), Address: 16/4, A-7, Anna Nagar, 4th Street, Kovilpatti 628501, Email ID: adityadonald476@gmail.com Contact Number: 6383256196

*Tumblr when they restricted sexual contents in their own platform. Thus, various social media apps come up with community guidelines which are very different from each other. In this article, we will explore about the level of restrictions on nudity and sexual contents by social media platforms and their responsibility in regulation of such acts with the guidance of Information Technology Act.*

## Introduction

The 21st century is an age of social media. Social media had a vast growth and its influence on people is very powerful. Global communication has undergone a transformation since the introduction of the internet and new media, which are defined by social networking sites like Facebook, Twitter, Instagram, and WhatsApp. The potential of social media messages to instantaneously and simultaneously reach a large, diversified audience and possibly influence their way of thinking and way of life is what gives them their greatest power. Article 19(1)(a)[3] of the Constitution guarantees freedom of speech and expression. However, the same is not absolute and is subject to the reasonable restrictions as provided in Article 19(2)[4]. In addition to being required by human nature, a civilized society demands that the State put certain reasonable restrictions on this particularly secured constitutional right. One among the restrictions imposed under Article 19(2) on this freedom is the 'decency and morality' with an objective to make sure that people's minds should not be corrupted.

Social media is a channel for the quick, personal, and interactive exchange of ideas amongst people all over the world. It also makes communication between them easy and effective. Due to the lack of effective management and control over the internet's flow of various types of content, this 21st century method of information exchange presents a challenge. The act of posting and disseminating obscene content on social media sites has generated controversy all around the world. The notion of obscenity differs

3 Constitution of India, 1950, Article 19(1)(a), Act of Parliament, 1950 (India).

4 Constitution of India, 1950, Article 19(2), Act of Parliament, 1950 (India).

and is not the same everywhere. What is obscene at one place or one time or to one person may not be obscene at the other. So the concept of obscenity varies from place to place, time to time and from person to person. In the case of Regina v. Hicklin[5], the word obscene was defined as "Any issue which tends to debase or degenerate those whose psyches are interested in corrupt impact." In the case of Ranjit Udeshi v. State of Maharashtra[6], the Supreme Court built up an adjusted adaptation of the Hicklin test as the test for indecency in India.

The capacity of social media messages to instantaneously and simultaneously reach a large, diversified audience and maybe influence people's way of thinking and way of life is what gives them their greatest power. Social media makes it easy for everyone to see the decline of etiquette and dignified ideals. When robbery, massacre, lawlessness, nakedness, and obscenity are the norm, politeness, nobility, and chastity have been declared 'No Go Zones'. In this context, obscenity is defined as the outrageous, offensive, and indecent portrayal of words or offensive images of victims of violence, murder, kidnapping, or sex-related details. Obscene and vulgar language is also used to describe public acts that deprave or corrupt the mind, appeal to the prurient interests, or violate accepted social moral standards. In recent years, the media has been largely responsible for propagating obscenity through semi-nude advertisements, videography, and news presented as soft-porn, and other means. For increased circulation, reading, viewership and money, they are unquestionably jeopardizing the morals of an entire generation. In this context, preventing the circulation of obscene material in social media becomes an important aim and the Government through various legislations strive to prevent the circulation of the same and to ensure proper, peaceful and better use of social media platforms without any hesitation or fear.

5 Regina v. Hicklin, L.R. 3 Q.B. 360 (1868).

6 Ranjit Udeshi v. State of Maharashtra, AIR 1965 SC 881.

## Obscenity Under Information Technology Act and Other Laws

The liberal-feminist sector of the society has frequently criticized the actions of Government under the pretext that the law on obscenity is vague. There have been numerous instances where law enforcement agencies have taken action against social media influencers or random people who have posted objectionable content on social media. On the other hand, content providers are observed producing obscene content under the guise of freedom of expression in exchange for cheap attention, a few Likes, and comments on their postings. These content producers prioritize making money from people who view their work.

The main aim behind the policies of the Government in the context of internet usage and social media is to ensure an Open, Safe and Trusted and Accountable Internet for its users. The definition of the term "obscene" or "obscenity" is neither provided in the IT Act nor in the Indian Penal Code. However, the wordings of section 67[7] of IT Act and section 292[8] of IPC explain obscenity as "anything which is lascivious or appeals to the prurient interest or if its effect is tend to deprave and corrupt persons." Publishing or transmission of any material which is sexually explicit through electronic form has been penalized under sections 67A[9] and 67B[10] of the Information Technology Act, 2000 which is punishable with imprisonment up-to three years and five years respectively. This offence is made a cognizable offence through section 77B[11] of IT Act.

To help in achieving the aim as mentioned in the above-mentioned paragraph, the Central Government through exercising the power given to them under the IT Act, enforced the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. These rules place a

7 Information Technology Act, 2000, S. 67, Act of Parliament, 2000 (India).

8 Indian Penal Code, 1860, S. 292, Act of Parliament, 1860 (India).

9 Information Technology Act, 2000, S. 67A, Act of Parliament, 2000 (India).

10 Information Technology Act, 2000, S. 67B, Act of Parliament, 2000 (India).

11 Information Technology Act, 2000, S. 77B, Act of Parliament, 2000 (India).

specific duty of care on intermediaries including social media intermediaries and state that if they fail to uphold this duty, they will no longer be immune from legal liability for any third-party information, data or communication connection they host.

Obscenity is also made an offence under the Indian Penal Code. Section 292 prohibits the sale or publication of any obscene pamphlet, book, paper, painting, and other such materials. Despite being a bailable offence, Section 293[12] criminalizes the sale or distribution of obscene objects to anyone who is under the age of 20, or an attempt to do so. Section 294[13] prohibits obscene acts and songs in public spaces. Obscene portrayal of girls or women is made an offence under the Indecent Representation of Women (Prohibition) Act 1986. Section 2(c)[14] of the Act defines obscene portrayal of girls/women as "the delineation in any way of the figure of a girl or women, her frame or body or any part thereof so as to have the impact of being disgusting, or slanderous to, or stigmatizing, ladies, or is probably going to debase, degenerate or harm the general population morale quality or ethics." This Act forbids the distribution or mailing of any books, handouts, slides, films, compositions, drawings, paintings, photos, portrayals, or figures in any shape that contain obscene portrayals of a girl or women. It also forbids the production, show, ads, deliver or cause to be created, deal, let to contract, distribute, or circle containing such depictions of girls or women.

## Social Media Obscenity and its Community Guidelines

Though there are several social media platforms which are available for public access, the most used significant social media intermediary apps are Facebook, Instagram, WhatsApp, Telegram and Twitter. Now let us have a close look on the degree of strictness of the community guidelines regarding obscenity and sexually explicit contents in their own respective social media platforms.

12 Indian Penal Code, 1860, S. 293, Act of Parliament, 1860 (India).

13 Indian Penal Code, 1860, S. 294, Act of Parliament, 1860 (India).

14 Indecent Representation of Women (Prohibition) Act, 1986, S. 2(c), Act of Parliament, 1986 (India).

Facebook: The Facebook community guidelines are pretty strict regarding their community guidelines relating to obscenity and sexually explicit contents. Facebook does not permit nude images even if it is artistic or creative in nature. This includes photos, videos and some digitally-created content that show sexual intercourse, genitals of male, female & other genders and close-ups of fully-nude buttocks. It also includes some photos of female nipples, but photos in the context of breastfeeding, birth giving and after-birth moments, health-related situations (for example, post-mastectomy, breast cancer awareness or gender confirmation surgery) or an act of protest are allowed. Nudity in photos of paintings and sculptures is allowed too[15]. That goes without saying that anything which is even remotely near to pornography would not be tolerated according to the community guidelines of Facebook.

For safety reasons, Facebook might remove images that show nude or partially-nude children. Even when this content is posted and shared with good intentions, this act is done by Facebook to avoid misusing the contents for unanticipated ways.

Instagram: The community guidelines of Instagram and Facebook are exactly the same as Instagram was acquired by the founder of Facebook (Mark Zuckerberg) a few years ago.

Telegram: Telegram prohibits the user from posting illegal pornographic content on publicly viewable Telegram channels, bots etc. It has all the rights to issue a ban on the channel if it has been reported for circulation of illegal pornographic materials.

WhatsApp: Though WhatsApp does not restrict the viewers from sending or circulating nude or sexually explicit contents, it is relatively safer than other social media platforms as it is a private circle. Unlike other social media apps, WhatsApp does not require User ID and Password. It is operated through the mobile number which is activated by the mobile phone in which

15 FACEBOOK, https://www.facebook.com/help/477434105621119, (last visited, Feb 21, 2023).

the sim card is situated. Unlike other social media apps, a person cannot log in WhatsApp from multiple devices. This provides a minimum security as people don't share or exchange their personal mobile number with strangers or unreliable people. The consumption and circulation of nudity as well as sexually explicit contents in WhatsApp is relatively lesser because people consider WhatsApp as a private medium which is predominantly used for chatting. There are a few WhatsApp groups which exists for the sole purpose of circulating nudity and sexually explicit materials. However, it is not seriously considered by WhatsApp as it does not affect children and general public. It is private and not easily available for the consumption of general public.

Twitter: Twitter has a relaxed community guidelines when it comes to nudity and sexually explicit contents when compared to other mainstream social media platforms. Twitter allows nudity and pornographic contents if it has the consent of the people involved added with a warning option to be marked as a sensitive content. It does draw a line when it comes to revenge pornography (Posting or sharing explicit images or videos that were taken, appear to have been taken or that were shared without the consent of the people involved). It also prohibits from sharing child pornography and other adult contents within live video or profile or header images. The explicit content indicating that it should be watched in private is widely known as NSFW (Not Safe for Work). Twitter has a feature to directly connect a user's OnlyFans (An online platform where people pay for contents such as photos, videos and livestreams which is mostly sexual or pornographical in nature) account to their twitter profile. This gesture arises a strong doubt that whether twitter knows about the hazards of this issue and wilfully neglects it.

Despite the lenience, Twitter stated that the following acts will be removed by them if someone reports the content

- Creepshots or up skirts;
- Content where a bounty or financial reward is offered in exchange for non-consensual nudity media; and

- intimate images or videos that are accompanied by text that wishes/ hopes for harm to come to those depicted or otherwise refers to revenge

  e.g., "I hope you get what you deserve when people see this"; and information that could be used to contact those depicted

  e.g., "You can tell my ex what you think by calling them on 1234567890"[16]

## Significance of this Issue

This issue needs to be addressed without further delays because of several reasons.

- Access for Children: In the modern era of smartphones, kids are more into social media platforms and they tend to spend most of their free time in it. In that case, the CEOs of every social media platform is responsible to restrict sensitive contents from reaching the eyes of children. It's preposterous to think that each and every single post must be checked and verified before it gets posted but in worst case scenarios, these platforms must at least try to remove the unwanted contents as soon as possible
- Convenient porn: In 2022, The Department of Telecommunications (DoT) has ordered Internet service providers to block more than 60 websites containing pornographic material in India. The orders are based on judgments issued by two High Courts and for violating the Information Technology (IT) Rules, 2021[17]. This raised the difficulty level in consuming pornographic contents in India. Certainly, there are other hacks to consume porn Illegally in India but it is not that

16 TWITTER, https://help.twitter.com/en/rules-and-policies/intimate-media, (last visited, Feb 21, 2023).

17 India porn ban: Government blocks over 60 additional websites, check the full list, INDIAN EXPRESS, (Feb 22, 2023 8:30 PM), https://indianexpress.com/article/technology/tech-news-technology/indian-govt-porn-websites-ban-full-list-8181130/

easy and familiar with most of the citizens. The relaxed restrictions in these social media platforms became a blessing for porn consumers. It became the most convenient method to access porn. This opened the floodgates for underage porn consumers.

- Easy to forge as an adult: Though these platforms has relaxed restrictions relating to nudity and sexually explicit contents, they do not allow some activities. One among the few is underage people accessing NSFW contents. However, the restrictions are not strict enough. As there is no proof required to prove the real age of the users, any person can hide their real age and enter a date of birth which seems to project them as adults. This little hack due to the lack of seriousness resulted in underage sexual content 'Creators' let alone underage sexual content 'Consumers'.
- Failure of Warnings: Even when a person is posting and sharing a consensual explicit content, it is mandatory to provide a warning that particular content which is about to be seen by a fellow user, contains sexual or violent contents in the post if any. However, this rule is not seriously taken neither by the social media platforms nor by the users. Sadly, the platforms do not care to take a peek into this issue.

## Suggestions

It is obvious to state that there is a very pressing need to balance the unnecessary curb of freedom of speech and expression and unnecessary spread of sexual obscenity, sexually explicit content which depraves the minds of individuals and prevention of online sexual crimes in the country. Therefore, the authors would like to put forth the following suggestions to achieve the same more effectively.

Firstly, the enactment of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 is definitely a good start to achieve the objective. Additionally, with regards to community guidelines of social media intermediaries, it is suggested that there is a need for a unanimous guideline for all social media intermediaries specifically

for the purpose of fixing the extent of sexually explicit contents that can be allowed to be published through the intermediaries. Hence, a single clear set of rules are to be made with reference to the same for all kinds of social media intermediaries.

Secondly, it is evident that there are options in almost every social media intermediary to block and report a content which is obscene or sexually explicit. But practically speaking, when a post is reported as being a revenge pornography or obscene or sexually explicit, the same is not taken down immediately. The process to assess whether such post is obscene takes at least few days. Moreover, generally for a post to be taken down, it requires report from at least a few accounts as a precondition. In this note, it is suggested that, the social media intermediaries shall be directed to make sure that there is a temporary pause option where such revenge pornography or sexually explicit content is kept on hold and not published until a proper decision has been arrived as to its true nature. If it is found to be harmless and proper, the publication of such post/content shall be resumed as it was before such pause. It is also understandable that creation of such an option leads to its misuse also and therefore action against such misuse is also to be formulated.

Thirdly, a drawback in the mechanism of age verification is that it is done through checking the email ID of a person where an email with a fake age can easily be created by anyone. Therefore, with an intention to make sure that such obscenity and sexually explicit contents does not reach the eyes of under age children, age verification shall be made not through email but through properly uploading a valid ID so that it can be made sure that access to such content is made available only to people belonging to age above 18. It is pertinent to make sure that, when such an ID is uploaded for the purpose of age verification, the social media intermediary shall make sure that the information of the ID is used only for such purpose thereby maintaining strict confidentiality and shall not be used or disseminated to others for purposes other than age verification. If the intermediary acts in contrary to this, they shall be made liable under the relevant provisions of

Information Technology Act and Indian Penal Code. Through this, contents generally shall be made available to all the accounts irrespective of any condition but age restricted contents shall be made available only to accounts which are properly verified through the above-mentioned process.

Though the above suggestions are not an exact solution to achieve the objective, it shall definitely be a stepping stone to achieve the same. Certainly, the above-mentioned methods will have an impact at least for an extent on the society and children.

## Conclusion

The most fundamental inherent right granted to its people by the 'basic law of the nation' is the 'freedom of speech and expression,' through which a person can express his or her feelings, thoughts, views, opinions, and sentiments, among other things, to others. The Indian Constitution's founders placed a high value on the right to free speech and expression. Decency and morality are two restrictions placed on this fundamental liberty[1]. The prohibition is based on the idea that the public mind shouldn't be tainted. Obscenity is not a universally accepted term. What is offensive in one place might not be offensive in another.

It can easily be said that more than half of the obscene material over the internet is in the form of revenge pornography. On one hand, curbing obscenity does not violate speech and expression of people but on the other hand, obscenity if not prevented, will violate the fundamental right to privacy of many people in the country and around the world. The significance over the curb of obscenity over the social media platforms lies over the fact that in recent times, usage of social media intermediaries is more prevalent among teens and children. Hence, obscenity over these platforms deprave the minds of the growing generation or the future of the nation, let alone grown adults. Further, revenge pornography, obscenity and mainstream pornography create a negative conception or a misconception about sex and body parts/image among people, particularly in the minds of teens and kids.

1 Ibid, 2.

Obscenity, though subjective, is a very serious menace to the society in the present as well as in the long run. Through this paper, the authors try to stress enough upon the seriousness of the issue of obscenity over the internet especially in social media platforms like twitter etc. The State and the Centre are striving to curb the same and this paper is intended to be of a clarificatory and helpful nature to hasten the goal.

# Rising Tides of Cyber Terrorism

***Malavika Anil[1] & Rahumath[2]***

## Introduction

*"An invasion by armies can be resisted but not an idea whose time has come. Infact, nothing is more powerful than an idea whose time has come"*

- Victor Hugo

Cyber terrorism is such an idea which have the capability to destroy the world without any invasions or armies or any military forces.

The computers and internet play a tremendous role in in our daily chores so the terrorists or criminals my take it as a preferred tool for attacking their targets. Nowadays internet is acting as a virtual battlefield for countries that have problem with each other such as Palestine and Israel, India and Pakistan, and many others. In a modern society this transformation from the traditional means to electronic methods are creating more problems. As the act of terror transferred from the physical world to the virtual world it become more dangerous. In case of present scenario there are many disturbing things happening in the virtual world or more precisely the cyber space. Now the internet and terrorism are interconnected, and it act as a

1 Student, CSI Institute of legal studies, Tvm

2 Student, CSI Institute of legal studies, Tvm

forum for the terrorist or their groups to spread their idea of hatred and violence and communicate it to large masses.

The cyber terrorism is an international threat. In addition to warfare on the physical world like air, water and land the cyber terrorism made cyberspace a dangerous battlefield. As being a border less environment the terrorist activity in this space is much more dangerous. That is the reason why international organisation like United Nations began an institution called United Nations office of counter terrorism or UNOCT. It had not only taken various measures to prevent cyber terrorism but also, they initiated a project that uses social media platform to gather digital evidence to counter the terrorism that is occurring through the cyberspace. In 2019 the United Nations secretary general Antonio Guterres stated cyber terrorism as a "new frontier" and further stated that terrorism is the denial of human rights, and the United Nations should take necessary measures to counter the terrorism.

By analysing the current trend of cyber terrorism, we are here to discuss the definition and concept of cyber terrorism its evolution throughout the years, about the cyber terrorist, recent and landmark incidence of cyber terrorism also about the national and international mechanisms to prevent cyber terrorism including case laws. The basic idea is to provide a detailed analysis about cyber terrorism and cyber security.

## Cyber Terrorism, Concept and Definition

As the term cyber terrorism does not have any proper definition many jurists along with other organisations have given their own explanation to the par term.

According to Black's law dictionary, defines cyber terrorism as the act of "Making new viruses to hack websites, computers and networks".

The FBI defined cyber terrorism as "The premeditated, politically motivated attack against information, computer systems, computer programs and data which result in violence against non-combatant targets by sub national groups or clandestine agents."

National Infrastructure Protection Centre or NIPC has defined cyber terrorism as "A criminal act perpetrated by the use of computers and telecommunications capabilities resulting in violence, destruction and /or disruption of services to create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government or population to conform to a political, social or ideological agenda[3].

North Atlantic Treaty Organization also known as NATO stated about the term as "sufficient destruction to generate fear or to intimidate a society into an ideological goal"[4].

In general, the political attack on the information system with proper planning for a malicious motive that is with an intention to harm any nation or any person for satisfying their own personal motive is called cyber terrorism.

Nowadays cyber terrorism usually overlaps with the terrorism even though it does not include any bloodshed, many researchers who have their research in terrorism proclaimed that cyber terrorism is not actually terrorism, but it is said to be hacking or an information warfare. According to many scholars' cyber terrorism must be used as a substitute for cyber warfare. Many security experts believe that if a cyber-attack or a crime creates a disruptive fear in people then potentially it can be called cyber terrorism. It is a dangerous collaboration between the internet and terrorism. We know that terrorism itself is a threat to our society when it is done through a medium that is accessible to all at a relatively small cost. The terrorism through this medium will have double the impact than that which happens in physical mode.

## Evolution of Cyber Terrorism

From early 1990, itself there was a notion of cyber terrorism. As the National Academy of science at that time stated that "we are at risk

3 WHAT IS CYBER TERRORISM, available at http://www.laweyerd.in (visited date February 20 2023)

4 CYBER TERRORISM AND VARIOUS LEGAL COMPLIANCES, available at, http://www.legalserviceindia.com (visited date February 23 2023)

increasingly America depends on computers…. Tomorrow terrorists may be able to do more with a keyboard than with a bomb". The situation is now more dangerous than that which is stated by the National academy of science. Being a borderless platform, it is difficult to control the activities happening in that space. Evolution of cyber space

The Barry c Collin coined the term cyber terrorism for the first time in 1990s but as 2000s approached the cyber terrorist were given with more and more potential.

Some of the important events that explains the evolution of cyber terrorism includes the one that happened in 1998 in Sri Lanka when the Tamil guerrillas tried to attack the Sri Lankan embassies by sending a ton of email to the embassies approximately 800 mails were received by them in a day for two weeks. The mail quoted nothing but a statement that is "we are internet black tigers; we are doing this to disrupt your communication" this is characterized as the first ever terrorist attack in cyber space against a country by the intelligence authority. Similarly in 2015 a person named Ardit Ferizi who was a citizen of Kosovo was punished for 20 years as it was found out that he has some affairs as he provides a material support to the prohibited organization of Islamic state of Iraq and levant. He provided ISIS with a data of 1300 military personnel so that it can help ISIS with the attack. He collected the data by hacking into the protected computer networks. The United States convicted and punished him. Kane Gamble another person who was arrested for leaking the confidential information from FBI, department of justice. he was a UK citizen and was convicted on 2018. He gains access to the computer network by impersonating the chief of CIA. This all events resembles how the cyber terrorism has been evolved and their recruitment strategy which is causing future threat to the world[5].

5 HOW CYBER ATTACKS ARE EVOLVING www.bankinfosecurity.com available on (February 23 2023)

## Perceived Risk of Cyber Terrorism

Cyberterrorism straddles the line between being a real bomb and not being as dangerous as one. Even if the threat of cyberterrorism may not seem as serious as it first appears, maintaining national security is at stake. Being politically motivated, cyber terrorism is more interested in destroying the nation's vital infrastructure, which has an indirect impact on the general populace by disrupting the financial and commercial infrastructure. Security concerns from cyberterrorism are quite serious. The Computer Infrastructure System (CIs) are dependent on cyberspace, just like nuclear sites, electricity grids, air surveillance systems, financial markets, and banking networks. This functional reliance has made CIs more susceptible to cyberterrorist attacks and significantly expanded the potential for cyberterrorist footprints. Most CIs globally are poorly protected. Therefore, cyberterrorism attacks on CIs can cause egregious damages to the society. Further, today there is a persistent threat of sensitive information of national interests being stolen by terrorists, destruction of computer networks or systems superintending the functioning of CIs.

### *Exploitation of Cyberspace by Terrorist*

Cyberspace is used by terrorist organisations for recruiting, command and control, and the dissemination of their ideologies. The fact that the Internet is the world's largest knowledge source has encouraged terrorist organisations to take use of this attribute and establish virtual training facilities in cyberspace. Al-Qaeda launched its first digital information hub in 2003, offering resources on everything from bomb-making to survival techniques. Today, many self-radicalised supporters use the Internet as a resource repository. By adding new dimensions to cybersecurity by preventing online terrorist recruiting, radicalization, and fund-raising, cyberspace has evolved as a new operational environment for terrorist and extremist organisations. With the addition of additional aspects to cybersecurity, cyberspace has become a new operating environment for organisations supporting terrorism and extremism. This prevents online

terrorist recruitment, radicalization, and fund-raising. This tactic has been skilfully manipulated and applied by the IS terror group for its own purposes. Social internet helped the terrorist group sign up 30,000 new members as warriors. Social media later aided the organisation in establishing its franchises and growing its clientele across the globe. Also, terrorists use their knowledge of the Internet to communicate with the public in order to spread their messages and encourage acts of terrorism[6].

### *Cyber Terrorism Threat in India*

There have been many shocking internet war incidents against this country. But, we continue to see that we are largely unprepared to defend against the cyberattacks by China and Pakistan against our country India. Earlier this year, a Swedish "ethical hacker" exposed the email addresses and passwords of several Indian government institutions, including the National Defence Academy and the Defence Research and Development Organization. This incident is significant in light of China's ongoing development of its electronic warfare capabilities as well as its quick (and opaque) modernization of its military. In an effort to add a new layer of complexity to the ongoing Indo-Pak confrontation over Jammu and Kashmir, hackers from Pakistan and terrorist groups are stepping up their attacks on Indian websites. The terrorist groups were turning to the internet and information systems to expand their conflicts into entirely new terrain and give them a new, low-cost dimension with maximum impact. Particularly over the past few years, Pakistani hacker groups like Pakistan Hacker Club have increased their attacks against Indian websites.

Being neighbours there always arise tension between India and Pakistan over Kashmir. The cyber hackers and terrorists from Pakistan tried to attack the internet community of India. Prior to or after 11th September it is believed that the al Qaeda organisation and other sympathisers of Pakistan started to spread their propaganda over the internet community of India.

6 CYBER TERRORISM AND LAWS IN INDIA available at https://www.legalserviceindia.com visited on (February 23 2023)

Certain groups even disrupted the service of many large entities like Zee TV network, Bhabha atomic research centre etc. The hacker's groups from Pakistan also tried to target the United States air force computing environment and department of energy website[7].

## Methods of Cyber Terrorism

### *Privacy Violation*

The law of privacy recognises a person's right to seclusion and an unfettered personal space. But, in recent years, this right has gained constitutional protection, and now anyone who violates it faces legal repercussions on both the civil and criminal levels. The intensity and complexity of life have made some sort of withdrawal from it imperative. As a result of culture's reshaping impact, man has developed a sensitivity to visibility, making isolation and privacy crucial to the person. The right to privacy is a component of the rights to life and to personal liberty guaranteed by Article 21 of the Indian Constitution. The conventional notion of the right to privacy has undergone new iterations with the development of information technology.

### *Demolition of E-governance*

E-governance aims to make interactions between citizens and government agencies simple and to promote open, free exchange of information. It furthers the realisation of the right to relevant information. In a democracy, citizens govern themselves, and for them to do so effectively, they must be informed of the social, political, economic, and other concerns that are at stake. They need access to a variety of viewpoints on those topics in order to be able to judge them properly. Free speech includes the implicit right to receive and impart knowledge. Nonetheless, this right to information is not absolute and is subject to reasonable limitations that the government may apply when doing so is in the public interest.

7 Supra no 2

### *Distributed Denial of Service Attack*

The Government and its agencies' electronic bases may be overloaded by cyberterrorists using the distributed denial of services (DDOS) technique. This is made possible by using viral attacks to first infect a number of vulnerable computers before seizing control of them. Once under charge, the terrorists can manage them from any location. These infected computers are then programmed to send information or make requests in such a volume that the victim's server crashes. Furthermore, because of this superfluous Internet traffic, legal traffic cannot reach the computers of the government or its agencies. The government and its agencies suffer a great financial and strategic loss as a result.

### *Network Deterioration and Disruption*

The fundamental objective of cyberterrorist actions is to harm networks and disrupt them. The security authorities' focus may temporarily be diverted by this activities, providing the terrorists more time and making their job relatively simpler. This procedure might combine hacking, viral attacks, computer tampering, and other activities[8].

### *Legislations Governing Cyber Terrorism in India*

The Information Technology Act, sometimes known as the Act, authorises laws pertaining to cyber terrorism. The Act's Section 66F establishes a framework for law enforcement to combat cyberterrorism. Along with three requirements for an act to qualify as cyberterrorism, it stipulates penalties for the crime up to and including life in prison.

- **Intention:** The act must intend to afflict terror in people's mind or jeopardise or endanger the unity, integrity, security or sovereignty of India.
- **Act:** The act must cause:

8 CYBER TERRORISM IN INDIA available at https://www.jcreview.com (visited date February 24 2023)

(i) unlawful denial of access to any legally authorised person from accessing any online or computer resource or network.

(ii) unauthorised attempt to intrude or access any computer resource; or

(iii) introduce or cause to introduce any computer contaminant.

- **Harm:** The act must also cause harm, like death, injuries to people, adverse or destructive effect on the critical information infrastructure (CII), damage or destruction of property or such disruptions likely to cause disturbances in such services or supplies which are essential to life.

***Indian Computer Emergency Response Team ("CERT-In")***

According to Section 70B of the IT Act, the CERT-In team was established to offer timely alerts of incidents posing a threat to cyber security as well as a list of emergency procedures for dealing with those situations.

***National Cyber Security Policy***

India's National Cyber Security Policy, which was published in 2013, intends to protect Indian cyberspace and strengthen the country's ability to fend off threats in all industries. It intends to provide strategies for safeguarding India's CII as well as procedures for efficiently fending off cyberattacks. It also emphasises on a trustworthy and secure cyber ecosystem in India.

With the help of the policy, a secure computing environment has been created, and extraordinary trust and confidence in electronic transactions have grown. Furthermore, a crisis management plan has been instituted to counter cyber-enabled terror strikes. Also, the National Investigation Agency (NIA) Act was modified by the Parliament in 2019 to enable the NIA to look into and prosecute instances of cyber terrorism.

Technology and threat intelligence also play important roles in the fight against traditional and cyber terrorism. The multi-agency centre (MAC) at the national level, established after the Kargil intrusion, as well as satellite

MACs (SMACs) at the state level, have been upgraded and reorganised to enable them to operate on a 24x7 basis. Every organisation active in counterterrorism is a member of the MAC, which is made up of about 28 entities. This is just another crucial component of the national initiative.

Unlawful Activities Prevention Act, 1967

This Act establishes penalties for terrorist acts. Although cyber terrorism does not fit the criteria of terrorism as it is defined by this Act, this Act nevertheless specifies penalties for organising terrorist camps and recruiting people for terrorist acts. Utilizing cyberspace for the aforementioned purposes is also considered cyberterrorism and is therefore illegal.

## Combating Cyber Terrorism on a global scale[9]

### *Convention on Cybercrime*

The European Union's Convention on cybercrime, also called the Budapest Convention, is the sole binding international convention on cybercrimes. It aims at harmonising domestic laws, including an international cooperative framework, and also proposes to improvise investigation techniques on cybercrimes for member states. India is not part of this treaty.

Brazil, Russia, India, China and South Africa (BRICS) Counter-Terrorism Strategy.

The policy intends to combat global terrorism and its funding, strengthen collaboration between law enforcement agencies in extraditing terrorists and providing mutual legal help, among other things. The goal of the approach is to "fight extremist narratives supportive of terrorism and the abuse of the Internet and social media for the aim of recruiting, radicalising, and inciting terrorists."

9 CYBER TERRORISM: A TOOL OF MASS DESTRUCTION, available at https://www.ijmh.com (visited date February 24 2023)

### *UN Global Counter-Terrorism Strategy*

The plan demonstrates the dedication of all UN member nations to the elimination of terrorism in all its forms. The resolution strives to prevent the spread of terrorism via cyber networks and to increase international and regional collaboration and coordination among nations, business actors, and others in the fight against cyber terrorism. The member states are urged to make sure that internet "is not a safe haven for terrorists" in the 2018 resolution regarding the sixth review of the strategy. Member states are urged to combat terrorist propaganda, provocation, and recruiting, including through cyber space[10].

## Conclusion

The very nature of terrorism is an insurmountable phenomenon that has troubled humanity for terrorism. Moreover, with the impact of modernity terrorism, has taken shape in the form of modern terrorism. A modern terrorist is now capable of wreaking devastation sitting in an unknown location using just a mouse and keyboard rather than any traditional means, save from the lone wolf attack, which is also a new phenomenon.

Without regard to national or regional boundaries, the internet has evolved into a decentralised network of communication. Thus, effective cyber terrorism management requires global regulation and a cooperative cybersecurity architecture. It is necessary to strengthen international law in order to prepare it to cope with cyberterrorism because the current framework is unable to contain the threat. Also, India should consider updating its current legal system or enacting specialised cybersecurity legislation that might include measures for cyberterrorism.

In the modern world, India's economic, business, and other interests connect with cyberspace. At all levels of operation, the union must implement strict deterrence policies and cybersecurity reforms in order to protect India's strategic, sovereign, economic, and business interests in

10 Id

cyberspace. When analysing cyber terror threats, it's important to consider the big picture. New mechanisms must be developed and reformative steps must be implemented, with a focus on the constitutional duty of the state under Article 19(1)(g) and Article 355 of the Indian Constitution. The laws have to take care of the problems originating at the international level because the internet, through which these terrorist activities are carried out, recognizes no boundaries.

The economic foundation of a nation can thus be destroyed by a cyberterrorist operating from a location with which that nation may not have reciprocal agreements, such as a "extradition treaty." The only safeguard we have is to combat these issues with the most recent technologies. As a result, we are aware that a law addressing cyber terrorism and the most recent security technology must work well together.

# Examining the Effects of Virtual Harassment and Violence on Female Students in Indian Higher Education

***R. Enitha[1] and R.G.Swetha[2]***

## Abstract:

*Women's safety has become a major concern and topic of discussion in India in recent times.Unfortunately, in India, victims of harassment are often blamed for the harassment they face,with their clothing or choice to go out alone at night becoming an excuse for the perpetrator'sbehaviour. This problem is not limited to physical environments but also exists in onlinespaces. Women frequently face unwanted advances, offensive emails, and rape threats in thevirtual world, especially in the context of online classes.*

*The COVID-19 pandemic has forced many professors and students to attend classes online,which has further exacerbated the problem of sexual harassment. Female teachers and girlstudents are at a higher risk of being subjected to sexual harassment during online classes,including the exchange of sexually explicit or provocative information and improper gesturesor remarks made by classmates or instructors. Societal expectations and cultural attitudes inIndia make women more vulnerable to this kind of harassment.*

*The rise in virtual interactions has made sexual harassment more prevalent in these pandemictimes. Online environments provide perpetrators with anonymity and the ability to easily findand target their prey. This has created a need for schools and institutions to establish explicit procedures and guidelines*

1& 2 SOEL,Tamil Nadu, Dr. Ambedkar Law University, Chennai, India

*for students to feels a fereporting and receiving support for incidents of sexual harassment.*

*Studies indicate that 83% of Indian women have faced some form of online abuse, and 70%have experienced an increase since the pandemic began. The study in question aimed toassess the problem of cyber violence against women and found that sexual harassment during online classes is awidespread issue in Indian educational institutions.There por trecommends the expansion of awareness campaigns, mandatory sexual education classes for new students, and there orientation offinal-year students to address the issue. It is essential to monitor the current situation and strengthen enforcement of existing legislation to combat theproblem of virtual harassment and violence against women in Indian higher education.*

## Introduction

India's higher education institutions have been a site of rampant virtual harassment and violence against female students, reflecting the larger patriarchal and gendered power structures in the society. With the increasing reliance on digital technologies for learning and communication during the COVID-19 pandemic, the issue has become even more pressing. Virtual harassment and violence take various forms, including cyber bullying, stalking, online sexual harassment, and non-consensual sharing of personal information or images. These actsof harassment and violence can lead to a range of negative consequences for female students, including anxiety, depression, lower academic performance, and even droppingout of education.

The issue is further compounded by the lack of adequate policies and mechanisms to address it, leaving female students vulnerable to repeated attacks and without sufficient recourse. Addressing virtual harassment and violence against female students is critical for ensuring anequitable and safe learning environment for all. It is important to understand the prevalence, forms, and impact of virtual harassment and violence to develop appropriate interventions and policies.

In a survey conducted by the Indian National Bar Association, it was found that only 14% of female students who experienced virtual harassment

and violence reported the incident, and only 8% of those who reported the incident received any support from their educational institution. This reflects the lack of adequate policies and mechanisms in place to address the issue and protect female students from further harm.

Here are some examples of case laws related to virtual harassment and violence against women in Indian higher education:

Vishaka and Others v. State of Rajasthan and Others, AIR 1997 SC 3011: This case dealt with the issue of sexual harassment of women in the work place and led to the development of guidelines to prevent and address sexual harassment. The guidelines, known as the Vishaka Guidelines, provide a framework for preventing and addressing sexual harassment in educational institutions as well.[2]

ShreyaSinghalv.Union of India, (2013) 12SCC73: This case challenged the constitutionality of Section 66A of the Information Technology Act, 2000, which criminalised certain online activities, including the posting of "offensive" content.The Supreme Court struck down the provision on the grounds that it violated freedom of speechand expression.[3]

Ankur Sharma v. Union of India and Ors., W.P. (C) 8686/2020: This case dealt with the issue of online sexual harassment and bullying in educational institutions and called for the development of guidelines to address the issue. The court emphasized the need to protect the privacy and dignity of students and prevent them from being subjected to online harassment and bullying.[4]

These case laws demonstrate the importance of addressing virtual harassment and violence agains two men in higher education and developing effective policies and guidelines to prevent and address such issues.

2 Vishaka and Others v. State of Rajasthan and Others, AIR 1997 SC 3011

3 Shreya Singhal v. Union of India, (2013) 12 SCC 73

4 Ankur Sharma v. Union of India, W.P. (C) 8686/2020 (Delhi High Court 2020

## Methodology: Research Design, Data Collection, and Analysis

### *Methodology*

The study utilized aqualitative research design, employing semi-structured interviews with 20 female students in Indian higher education who had experienced virtual harassment and violence. The sample was selected through purposive sampling, ensuring diversity in terms ofage, course, and type of virtual harassment and violence experienced.

### *Data Collection*

Data was collected through semi-structured interviews conducted over video conferencing platforms, ensuring the anonymity and confidentiality of the participants. The interviews were audio-recorded with the permission of the participants and later transcribed verbatim.The interviews focused on understanding the nature and impact of virtual harassment and violence, the coping mechanisms used by the victims, and their suggestions for a ddressing the issue.

### *Data Analysis*

The data collected through the interviews was analyzed using thematic an alysis. The transcribed interviews were coded by two researchers independently, and the codes were collated and grouped into broader themes. The analysis involved iterative coding, constant comparison, and refinement of themes until saturation was reached. The findings were presented through quotes from the participants to provide a richer understanding of the experiences of the victims of virtual harassment and violence in Indian higher education.

## The Prevalence of Virtual Harassment and Violence in Indian Higher Education

Virtual harassment and violence against female students in Indian higher education institutions are widespread issues. A study by the Indian

Journal of Psychiatry found that almost half of the surveyed female students experienced some form of virtual harassment or violence, including cyber bullying, online sexual harassment, stalking, and non-consensual sharing of personal information or images.

The prevalence of virtual harassment and violence is highlighted by the case of a DelhiUniversity female student who was threatened with rape and murder on social media platforms for speaking out against a political party's student wing. Due to the continuous harassment and lack of support from the university, the student eventually withdrew from her studies. Another case that garnered widespread media attention was the suicide of an Indian Institute of Technology (IIT) Madras student who had faced prolonged virtual harassment from a male student who posted derogatory comments and sent sexually explicit messages. The IIT Madras administration faced criticism for its lack of action and support for the victim.

The Indian government has introduced legislation such as the Information Technology Act, 2000, and the Sexual Harassment of Women at Workplace (Prevention, Prohibition, and Redressal)Act, 2013, to address cyber crime and online harassment. However, the implementation and enforcement of these laws remain a challenge.

In one case that exemplifies the legal recourse available to victims of virtual harassment, in the case of Mona Mathur v. State of Uttar Pradesh, Criminal Appeal No. 17 of 2019, a female college student was stalked, harassed, and eventually murdered by a man who had been stalking her both online and in person. Despite repeatedly complaining to college authorities about the stalker's behaviour, they failed to provide any protection or support. This case highlights the urgent need for colleges and universities to take harassment and stalking complaints seriously and provide adequate support to victims. It also underscores the importance of effective legal measures to address online stalking and harassment, which can escalateinto physical violence.[5]

5 Mona Mathur v.State of Uttar Pradesh, Criminal Appeal No.17 of 2019.

## The Forms of Virtual Harassment and Violence Experienced by Female Students

Female students in Indian higher education institutions experience various forms of virtual harassment and violence, which can have a serious impact on their mental health, academic performance, and overall well-being. The forms of harassment and violence experienced by female students in India include online sexual harassment, cyberbullying, stalking, and non-consensual sharing of personal information or images.

Virtual harassment and violence against females in Indian higher education can take many forms, including but not limited to:

1. **Cyberstalking:** This refers to the repeated use of technology to harass, intimidate, and threaten an individual. Cyberstalkers use various methods to track their victims, such as following them on social media platforms, sending unwanted messages and emails,and even creating fake profiles to gain access to personal information.
2. **Revenge porn:** This is the sharing of sexually explicit images or videos without the consent of the victim. Such images can be posted on social media platforms or sent directly to the victim or their family and friends, causing immense emotional and psychological distress.
3. **Online bullying:** This is the use of technology to humiliate, embarrass, and intimidatean individual, often through social media platforms or instant messaging services.
4. **Trolling:** This refers to the posting of inflammatory, off-topic, or abusive comments in online forums, social media platforms, and other public spaces with the intention of provoking an emotional response from the victim.
5. **Doxxing:** This is the release of an individual's private information, such as their homeaddress, phone number, and email address, with the intention of inciting harassment and violence against the victim.
6. **Hacking:** This refers to the unauthorised access to an individual's digital accounts, including email, social media, and banking accounts,

and using the information for malicious purposes, such as blackmail or identity theft.

The impact of virtual harassment and violence can be severe, leading to emotional and psychological trauma, socialisolation, academic and career setbacks, and even physical harm. It is essential to raise awareness about the different forms of virtual harassment and violence and take measures to prevent and address them.

One example of virtual harassment in India is the case of Shreya Singhal v. Union of India(2013). In this case, a law student challenged the constitutional validity of Section 66A of theInformation Technology Act, 2000, which allowed for the arrest of individuals for posting offensive or menacing messages on social media platforms. The Supreme Court of India eventually struck down Section 66A, stating that it was a violation of the right to freedom of speech and expression.[6] Another case that exemplifies the forms of virtual harassment experienced by female students is the case of Nandini Praveen v. The Principal, Kumaraguru College of Technology (2016). In this case, the victim was subjected to cyberbullying by her classmates, who had created a fake profile of her on a social networking site and posted derogatory comments and images. The victim was also physically assaulted on campus. The Madras High Court ordered the college to pay compensation to the victim and take appropriate action against the perpetrators. These cases demonstrate the various forms of virtual harassment and violence experienced by female students in India and the need for effective legal and institutional mechanisms to address the issue and provide support to victims.[7]

Virtual Harassment and Violence's Effect on Female Students' Academic Performance Virtual harassment and violence involve the use of electronic communication tools to bully, harass, or threaten individuals. Such

6 Shreya Singhal v. Union of India, (2013)12 SCC 73

7 Nandini Praveen v. The Principal, Kumaraguru College of Technology, (2016) 2 SCC 13

harassment can include cyberstalking, online threats, and negative comments. Virtual harassment and violence can affect the mental and physical health of victims. The impact on academic performance can be significant and long-lasting.

Some case law has shown that virtual harassment and violence can negatively impact the academic performance of female students. In the case of Sakshi Mishra vs. State of UP & Ors(2019), the court observed that the harassment of the petitioner had a severe impact on her mental and emotional well-being, which resulted in her inability to concentrate on her studies.[8]

Similarly, in the case of State of Punjab v. Jagir Kaur (2013), the court held that the victim's academic performance had been adversely affected by the trauma and mental agony caused by the harassment. The court also observed that the victim had been forced to drop out of school due to the harassment.[9]

Prevention and intervention are critical to addressing virtual harassment and violence against female students. Educational institutions should have clear policies and procedures for reporting and handling cases of virtual harassment and violence. The school's administration should also provide resources and support services for victims, such as counselling and legal advice. Education on digital citizenship and online safety should be incorporated into the school curriculum.

In the case of Amrinder Kaur v. State of Punjab (2016), the court held that educational institutions have a duty to provide a safe and secure environment for their students. The court directed the educational institution to establish a committee to deal with complaints of sexual harassment and provide counselling and legal support to the victims.[10]

Virtual harassment and violence have a significant impact on the academic performance of female students in India. It is essential to address

8 Sakshi Mishra v. State of U.P. & Ors.,W.P.No.11508 (M/B) of 2019.

9 State of Punjab v. Jagir Kaur,(2013) 4SCC1.

10 Amrinder Kaur v. State of Punjab, 2016 SCC OnLine P&H 4654 (India)

this issue and provide support to victims. Educational institutions should implement policies and procedures to prevent and intervene incases of virtual harassment and violence. By addressing virtual harassment and violence, female students in India can feel safer and more supported in their academic pursuits.

## Factors Contributing to Virtual Harassment and Violence Against Females in Indian Higher Education

The study identifies several factors that contribute to virtual harassment and violence against females in Indian higher education, including:

1. **Patriarchal attitudes:** Patriarchal attitudes that reinforce gender stereotypes and perpetuate the notion that men are superior to women, and that women should be submissive and obedient create a culture that normalises harassment and violence against women.
2. **Lack of awareness:** A lack of awareness about the different forms of virtual harassment and violence and their impact on victims can contribute to a culture of victim-blaming and trivialization of the issue.
3. **Cybersecurity:** The lack of cybersecurity measures, such as two-factor authentication, secure passwords, and encryption, can make it easier for perpetrators to gain access to their victims' accounts and personal information.
4. **Lack of institutional support:** A lack of institutional support from educational institutions, such as policies and procedures that prioritise the safety and well-being of female students, can make it harder for victims to seek help and feel supported.
5. **Cybercrimelaws:** In adequate cybercrime laws and the lack of a robust legal framework to tackle virtual harassment and violence can create a sense of impunity for perpetrators.
6. **Online anonymity:** The ability to remain anonymous online can embolden perpetrators to engage in virtual harassment and violence, as they feel protected from consequences.

It is essential to address these contributing factors to prevent virtual harassment and violenceagainstfemalesinIndianhighereducation. Thisrequires a multi-pronged approach thatincludes awareness-raising, institutional support, cybersecurity measures, and a robust legal framework to ensure accountability. Only by addressing these factors can we create a safe and inclusive learning environment for all students.

## The Impact of Virtual Harassment on Female Students' Psychology and Emotions

Virtual harassment and violence against female students can have a significant psychological and emotional toll, leading to anxiety, depression, post-traumatic stress disorder, and other mental health issues. Such harassment can also result in a sense of helplessness, low self-esteem, and a loss of confidence, affecting the overall well-being of the student.

One case that highlights the psychological and emotional toll of sexual harassment is the case of Bhanwari Devi v. State of Rajasthan (1996). In this case, the victim, Bhanwari Devi, a socialworker, was raped and sexually assaulted for opposing the child marriage of a one-year-old girl. The courtobserved that sexual harassment is not limited to physical advances but also includes verbal, non-verbal, and visual harassment that creates an intimidating, hostile, and offensive environment for women. The court acknowledged thesevere emotional and psychological impact of sexual harassment and recognised the right ofwomento work in an environment free from sexual harassment.[11]

Similarly, in the case of Mahak Rathee v. State of Haryana (2019), the victim was subjectedto online harassment and stalking by her former boyfriend. The court recognised the severe emotional and psychological trauma caused by such harassment and held that online harassment could have long-term and adverse consequences on the mental health of the victim.[12]

11 Bhanwari Devi v. State of Rajasthan,1996 SCC (2) 383

12 Mahak Rathee v.State of Haryana, (2019) 5 SCC 781

These cases emphasize the need for a safe and supportive environment for female students in higher education and the urgent need to address virtual harassment and violence to protecttheir psychological and emotional well-being.

## Coping Strategies of Female Students with Virtual Harassment and Violence

Coping mechanisms, like seeking support from friends and family, reporting harassment to authorities, and using online resources and tools, are crucial for female students affected by virtual harassment and violence. These mechanisms help to provide emotional support, hold perpetrators accountable, and protect the victim's privacy and safety.However, the effectiveness of coping mechanisms may vary from person to person, and therefore, it is necessary to provide a range of resources and support for victims to choose from.

In the case of Romila Thapar v. Union of India (2018), a group of women scholars challenged the arrest of five activists for allegedly inciting violence in Bhima Koregaon. The court observed that students and activists should be free to express dissent and criticism, and the state should not use its power to suppress legitimate expressions of dissent.[13]

This case highlights the importance of having a safe and supportive environment for students to express their opinions and views freely without fear of virtual harassment or violence.

Another case, M. C. Mehta v. Union of India (1997), focused on environmental activism and the right to a clean and healthy environment. The court acknowledged the significant role played by students and activists in raising awareness and advocating for environmental protection.[14]

These cases emphasise the need for a safe and supportive environment for female students in higher education to express their views and opinions

13 RomilaThapar v.Union of India, (2018) 10 SCC 753.

14 M.C.Mehta v.Union of India, (1997) 2 SCC 353

freely and the need for authorities to take effective measures to prevent virtual harassment and violence.

## Institutional Policies to Address the Virtual Harassment of Female Students

Institutions and policies have a significant role in addressing virtual harassment and violencein Indian higher education. It is important for institutions to have clear policies and guidelines in place to prevent and respond to such incidents and to provide support to affected students.

One such case is that of Ankur Sharma v. Union of India and Ors. (2020), in which the Delhi High Court directed the University Grants Commission (UGC) to issue guidelines for addressing complaints of sexual harassment in universities and higher education institutions.The court emphasised the need for the UGC to take a proactive role in preventing and addressing incidents of virtual harassment and violence.[15]

In addition, the Sexual Harassment of Women at Workplace (Prevention, Prohibition, and Redressal) Act, 2013, provides a framework for addressing sexual harassment in the workplace, including in higher education institutions. It mandates the establishment of Internal Complaints Committees (ICCs)to receive and address complaints of sexual harassment, and requires institutions to provide a safe and supportive environment for women.

The UGC also issued guidelines in 2015 on the prevention and redressal of sexual harassment in higher education institutions, which provide a framework for addressing sexual harassment and ensuring the safety and well-being of students.

These policies and guidelines, along with effective implementation and enforcement, canplay a crucial role in preventing and addressing virtual harassment and violence in Indian higher education.

15 Ankur Sharma v. Union of India and Ors.,W.P. (C) 3935/2017 (Del. HC 2020)

## Addressing Virtual Harassment of Female Students: Recommendations

Virtual harassment and violence against female students in Indian higher education is a pervasive issue that can have significant negative impacts on their academic performance and emotional well-being. As such, it is imperative that institutions and policymakers take stepsto address this issue and create safe and supportive learning environments for all students.

Basedonthefindingsofthisstudy,werecommendthatinstitutions:

1. Develop and implement comprehensive policies and procedures for preventing, reporting, and addressing virtual harassment and violence against female students.
2. Provide mandatory training to all students and faculty on recognizing and preventing virtual harassment and violence.
3. Increase resources for mental health and counselling services for students who have experienced virtual harassment and violence.
4. Foster a culture of respect and inclusivity on campus through awareness campaigns, workshops, and other initiatives.
5. Ensure that there is accountability for perpetrators of virtual harassment and violence through effective enforcement of policies and legal frameworks.

Addressing virtual harassment and violence against female students in higher education requires a multi-pronged approach involving legislative, institutional, and societal measures.

One way to address this issue is by strengthening the legal framework around it. For instance,the Sexual Harassment of Women at Workplace (Prevention, Prohibition, and Redressal) Act, 2013, can be amended to explicitly cover harassment and violence in the virtual realm. Additionally, universities can be mandated to adopt and enforce the University Grants Commission (Prevention, Prohibition, and Redressal of Sexual Harassment of Women Employees and Students in Higher Educational Institutions) Regulations, 2015.

In addition to legal measures, institutional measures can play a significant role in addressing virtual harassment and violence against female students. Universities and colleges must establish a zero-tolerance policy towards such behaviour and implement effective reporting mechanisms. They must also provide support and counselling services to victims and ensure that all complaints are dealt with swiftly and impartially.

While coping mechanisms are essential for individuals who have experienced virtual harassment and violence, societal measures are also necessary to address the root causes of this issue. Creating awareness and promoting gender equality in education and society can help prevent such incidents from occurring in the first place. Encouraging a culture of respect and empathy towards all individuals can help change societal attitudes towards virtual harassment and violence. It is essential to take proactive steps to prevent virtual harassment and violence by promoting healthy and respectful online behaviour and providing education and training on the responsible use of technology. Addressing the root causes of this issue canhelp create a safer and more equitable online space for everyone.

## Conclusions

Virtual harassment and violence against females in Indian higher education is a pervasive and insidious problem that has long-lasting impacts on the victims' mental health, academic performance, and future prospects. The study reveals that virtual harassment and violence can take many forms, including cyberstalking, revenge porn, online bullying, trolling, doxxing, and hacking, and can occur through various digital channels such as social media, messaging apps, and email.

It is evident that victims of virtual harassment and violence require support and protection from academic institutions, law enforcement agencies, and civil society. Educational institutions must implement policies that prioritise the safety and well-being of female students, provide awareness programmes, and offer counselling services to help victims cope with the trauma. Law enforcement agencies must take swift and decisive action

against the perpetrators of virtual harassment and violence, ensuring that they are held accountable for their actions. Civil society must also play a critical role in raising awareness about the problem and advocating for change.

In conclusion, combating virtual harassment and violence against females in Indian higher education requires a collective effort from all stakeholders. The issue is too complex to betackled by any one group or individual. Rather, it requires a coordinated and sustained effort from educational institutions, law enforcement agencies, civil society organisations, and individuals to create a safe and inclusive learning environment for all students.

# Freedom of Speech and Expression Through Internet and its Prohibition in the contemporary world

***Ms. Aswani S Dev[1] & Anju Simon[2]***

## Abstract

*India isthe largest democracy globally, with a population of 1.3 billion. Democracy is associated with the higher human accumulation and higher economic freedom. Democracy is closely tied with the financial source of growth like education, quality of life, and health care.The provisions related to freedom of speech and expression was included in the Constitution of India Bill of 1895, which is regarded as the earliest Indian expression of a constitutional vision. "Every citizen may express his or her opinions in writing and publish them in print without fear of retribution, but they shall be responsible for any abuses they may commit in exercising this right, in the instances and manner determined by the Parliament. "Accordingto the Supreme Court, the fundamental right, freedom of access to internet is safeguarded by Article19(1)(a) of the Indian Constitution, which guarantees freedom of speech and expression. Through this we can state that freedom of speech and expression is considered asone of the important tool in democratic country. We have an access to a worldwide platform and a quick means of communication, thanks to the internet. Early on, the internet was lauded as a new platform for unrestricted communication between individuals, free from the constraints of the "gatekeepers" who previously controlled the media's content. However, there is already a lot of discussion over the freedom of speech on internet, including whether it should be restricted, if it should be,*

1 & 2 LLM, National University of advanced Legal Studies

*and who should make the decisions about what is andhow it should be allowed. Beliefs or laws governing free speech will havean impact on awide range of aspects of ourlife. Due to their opinions on issues, speakers may be prohibited from speaking at universities or on any other public platforms. So through this paper we aregoing to look how freedom of speech and expression through internet is curtailed by our government through laws.*

## Introduction

In this modern era, the using of internet in our everyday lives is unavoidable. When used properly, the internet makes living quick, easy, and simple. The internet provides us with information, knowledge, and data that are useful for our personal, social, and economic growth. Although there are many uses for the internet, how we use it in our everyday lives depends on our own needsandobjectives. Due to the fact that it is fueled by internet research, the Internet is crucial to research and development.Both large universities and small business owners benefit from the internet. The internet is without a doubt the most effective form of communication available today. It quickly and cheaply connects individuals from different parts of the world. The internet has a significant impact on how we live ourlives. Without the internet, we would never have had the opportunity to explore the magical world of information it has unlocked for us. It is difficult to imagine a world without the internet given its size and significance. As the time passes internet became a source for expressing their ideas and thoughts in the cyberworld. As a result the opportunity for communication to a larger audience became possible.

The internet has strongly influenced our education system by connecting and empowering students and educators through unbounded possibilities of knowledge sharing and creating new ways of teaching and learning without the restriction of time and physical constraints that captivate and stimulate students' imagination at anytime, anywhere using an internet connected device. The internet can speedup growth, development and offer immense opportunities for strengthening the economy through e-commerce coupled with improved productivity and competitiveness as it has become

a major distribution channel for goods and services.[2] But internet also have its negative impact in the existing scenario. The traditional restrictions on free speech are defied by the virtual world, leading to brand-new issues that have not yet been solved. Social media's widespread use has prompted inquiries about how current legal standards and practices apply to ever-growing online territories. It has proven challenging to envision a predictable and transparent regime that safeguards online freedoms due to a number of issues and disputes.[3] When a person express his/her views in the cyberspace we can see that there freedom of speech and expression is curtailed. One of the biggest example is Kashmir (Internet Ban). Article 19 of our Indian Constitution provides Freedom of speech and expression, then also we can see that freedom of an individual to express there view is curtailed which is so dangerous in a democratic country like us. As we all know Indiais a democratic country we are considered to be the fathers of democracy.The right tofreedom of speech and expression belongs to every citizen. The three pillars of democracy—executive, legislative, and judicial—keep democracy in check, but in the modern era, democracy is leaning more toward the fourth pillar, the media.The said freedom is immensely important and the same can be figured out considering that media which has been considered the "Fourth Pillar of Democracy". Every citizen may express his or her opinions in writing and publish them in print without fear of retribution, but they shall be responsible for any abuses they may commit in exercising this right, in the instances and manner determined by the Parliament." This paper is based onthe freedom of speech and expression through internet and its prohibition in the contemporary world. The arguments center on whether the internet violates the right to free speech and expression or whether it makes that right absolute and exempt from all reasonable limitations.

2 Internet an Integral Part of Human Life in 21st Century: A Review | Current Journal of Applied Science and Technology (journalcjast.com)

3 FREEDOM OF EXPRESSION ONLINE from GOVERNING CYBERSPACE:A Road Map for Transatlantic Leadership on JSTOR

## Right to Freedom of Speech and Expression and its Restrictions

Citizens have the freedom to voice their opinions and criticize the government for its arbitrary actions thanks to the right to freedom of speech and expression. In a democracy, citizens elect their representatives to office through a voting process. The government is unable to impose monarchy rule in the state due to the right to free speech and expression. Incontrast to a democracy, a monarchy allows for the expansion of a single power across the executive, legislative, and judicial branches of government. The election of the government in a democracy depends heavily on the public's input. Additionally, it safeguards the nation's free and open press, which is the fourth pillar of democracy. Right is an integral component of the right to life under Article 21 of the Indian Constitution, according to the Supreme Court of India. The Indian Constitution's Article 19(1) is enforceable against the state in the event of a violation. According to Article 19(2) of the Indian Constitution, the right to freedom of speech and expression is not unrestricted but is instead subject to reasonable restrictions. The limitations are for the nation's security, sovereignty, and integrity as well as for friendly relations with other countries, public order, morality, and the prevention of hate speech, defamation, and court contempt. The limitations are put in place to protect the interests of the country and allow people to exercise their right to free expression responsibly and with caution.

## Right to Internet and its Violation in India

The internet has become one of the basic needs of people all over the world in recent decades.The variety of services the Internet provides its users can occasionally get them into trouble. The ability to express our ideas and opinions to others via the Internet does not, however,constitute a complete right to free expression in the online environment. The right to freedomof speech and expression is still subject to reasonable limitations. Article 21 of the Indian Constitution's Right to the Internet[2] was broken by the recent internet blackout in Jammu and Kashmir in 2019. In addition to violating

the residents of Jammu and Kashmir's rights to privacy and life under Article 21 of the Indian Constitution, the arbitrary suspension of internet services prevents them from exercising their rights to freedom of speech and expression under Article19(1)(a) and to trade, commerce, and business under Article19(1)(g). Additionally, it limits access to data related to Article19(1) of the Indian Constitution. The right to access the internet would become an unstated fundamental right under Article 19 of the Indian Constitution. An internet outage would then be considered aviolation of fundamental humanrights. Position of the Government on the Internet suspension become a huge discussion around the nation For a variety of reasons, the government frequently suspends internet service in Union Territories and States.The cause could be a major factor that causes chaos in the state, such as concerns about the security of the country or widespread disorder. Due to violations of Section144 of the 1973 Code of Criminal Procedure, the government shutdown the internet.

## Case Analysis

Jammu and Kashmir is a region of India that borders Pakistan and has been the focus of a protracted conflict between the two nations.[4] The territory was given special status and itsown constitution under Article 370 of the Indian Constitution, and Indian citizens from other states were not permitted to buy land or other property there. The Indian Government issuedthe Constitution(Application to Jammu and Kashmir) Order, 2019, on August 5,2019, which completely subordinated Jammu and Kashmir to all provisions of the Indian Constitution andremoved the special status it had held since 1954. In Anuradha Basin v. Union of India [5]the editor of the Kashmir Times Srinagar Edition, Ms. Anuradha Bhasin, filed the petition. The government, she claimed, forced the print media to "a grinding halt" by shutting down the internet, which is crucial for the modern press. She had

4 The constitution (application to Jammu and Kashmir) order, 2019

5 Anuradha Basin v. Union of India, ( 2020) SC,1725 (India)

not been able to publish her newspaper as a result since August 6, 2019. In addition, she claimed that the government did not evaluate whether the internet blackout was appropriate and proportionate to the goals it was pursuing. She claimed that law makers passed the restrictions under the impression that law and order would be in danger. Public order, however, differs from law and order, and neither were in danger when the order was passed.. Finally, the Supreme Court ruled that while reasonable restrictions apply, both the right to freedom of speech and expression under Article 19(1)(a) and the right to freedom of trade and commerce under Article 19(1)(g) online are constitutionally protected rights. The Supreme Court then went onto compare and contrast the proportionality tests used by Indian, German, and Canadian courts in great detail. When it came to resolving issues involving limitations on fundamental rights, it was discovered that while there was consensus that proportionality was the key tool to achieve judicial balance, there was no consensus that proportionality and balancing were interchangeable. The Court then explained how it interprets the proportionality test:

- The restriction's objective must be justifiable.
- The limitation must be required.
- The authorities must determine if there are any alternatives to the restriction.
- Only the least restrictive option should be used.
- A court must be able to review the restriction.

Based on the for egoing, the Court determined that:

1. India's Constitution protects the right to free speech and the right to engage in any occupation online.
2. The government had to demonstrate necessity and set a time limit in order to suspend Internet access, which it failed to do in this instance. In order to lift any suspension orders that were unnecessary or did not have a set duration, the government had to review them.

3. Restrictions under Section 144 of the Code of Criminal Procedure are subject to judicial review and cannot be used to stifle free speech. Thus, the State was mandated by the Court to review its limitations.

The Supreme Court of India ruled in K.S. Puttaswamy v. Union of India[6] that any limitations placed by the government on the freedom of speech and expression and the right to engage in any profession or occupation over the internet under Article 19 must meet the proportionality test. The government's decision is evaluated for reasonability using the proportionality test. The proportionality test is mentioned above.

The High Court recently ruled in Faheema Shirin v. State of Kerala and acknowledged that mobile phones and internet access through them are an integral part of daily life. The courtexamined resolutions passed by the General Assembly and Human Rights Council of the United Nations, both of which unequivocally highlight the importance of internet access in gaining access to information and its close connection to education and knowledge. According to the court, Article 21's fundamental rights to life, liberty, and privacy include the right to be able to access the internet. The court went on to say that it is a crucial component of the framework for freedom of speech and expression.

## Freedom of Speech and Internet – U.S. Analysis

***Freedom of Speech in America-***

America is a country which gives utmost importance to protection and expression and securing it. A wide interpretation of Freedom of Speech can be seen. Initially when we go deep into olden text of U.S we can see there was no provision for the protection of Freedom of Speech and Expression but soon realizing the importance of freedom of speech - The First amendment was amended which paved the way for the protection of speech and expression which states that – "Congress shall make no law respecting

6 Justice K.S. Puttaswamy (Retd) vs Union of India on 26 September, 2018, SC WRIT PETITION (CIVIL) NO.494 OF 2012

on the establishment of religion or prohibiting the free exercise there of or a bridging the freedom of speech or of press or to right of the people peaceably to assemble and to petition the government for a redress or grievances".[7] It has been added tobill of Human Rights

This amendment clearly states provides a clear cut protection of Freedom of Speech but it applies only to the congress. Supreme Court states that first Amendment provides protection which is expansive and includes wider ambit. In United States we can see that Freedom of Speech as a wider ambit and it is protected. It receives a high degree of constitutional protection.And together with that Judiciary had played a important role in the protection.

The Schenck v. United States[8] was one of the First Important case were supreme court were supreme court was first requested to strike down a clause which violated the Free speech Clause.

The two document which protect Freedom of speech are Bill of Rights and Written Constitution as Freedom of Speech is the most Fundamental Liberties against State Suppression. Before commencing in Human Rights Charter – England as declared it had fundamental Right. There are Four different Argument for Free Speech – (1) Arguments concerned with the importance of discovering truth, (2)Free Speech as an aspect of self-fulfilment,(3) The argument from citizen participation in a democracy,(4) suspicion of government.

(1) Arguments concerned with the importance of discovering truth – The free speech principle is very much important because it help sin finding or discovering the truth. If there is restrictions on speech then the truth will not comeout. The case which can be associated to it are John Straut Mill and it has played some part in the orizing of American Judges.

(2) Free Speech as an aspect of Self – Fulfilment – Free speech helps in the self –development and self- fulfilment of an individual.

7 http://constitution.congress.gov

8 Schenck Vs. United States, 249 U.S. 47

Restrictions on to it may limit the growth of an individual and limit on its personality. This theory states that freedom of speech is an independent good which helps in to growth of an individual.

(3) The argument from citizen participation in a democracy- A judgment in this case Whitley Vs California[9] and in another case Alexander Vs Meikle John[10] most of the United States argument are in associated to it states that primary purpose of the amendment is to protect the rights of citizens to understand the political issues inorder to participate effectively in the working of an democracy.

(4) Suspicion of government -All the other argument are in relation to the support of an free speech but this as an negative aspect it states that highlight the negative side of the government.[11]

One of the essential apect in the life of individual is communication and together with that protecting interest of people in communicating ideas and information and together with that to what extent audience are in interest in receiving the ideas. It is a claim that individuals have right to speech and it is the duty of the government to safe, secure and protect the need of an individual people Lee Bollinger, a leading commentary on the first amendment of united states argues that "Freedom of speech should be explained and defended as helping to develop a practise of tolerance".

***Freedom of Speech and Internet from U.S perspective-***

Internet has brought a lot of changes. Starting from the evolution of printing revolution the nto the evolution of web were a wide variety of information are easily available easy mode of transformation of information such as e-mail through net. In a U.S case Reno Vs American Civil liberties

9 Eric Barendt, Freedom of speech, Second Edition, Published by Oxford University Press, Indian Edition

10 Whitley Vs.Superior Court, L.A No.17793

11 William J. Brennan,The Supreme Court and Meikle John Interpretation of the First Amendment, Harvard Law Review, Vol.79,No.19 (Nov, 1965)pg1-20, http://www.jstor.com

union[12]– which talks about the mass speech yet developed? District Court and supreme Court states that it would be clear wrong to restrain speech on internet, except for the dissemination of obscene messages and of other material. The Reno case judgment was considered to be the most appropriate method of treating Internet. There as been certain regulation made to the Internet applies to Press.

One of the important discussion which was raised in Unites States is regard "Whether Internet should be regarded or treated in the public forum so that individual can claim access to it. But it was stated that access to net is organized by Private ISP. If an ISP denies an access to an individual or company there is no state action in it.

***Freedom of Speech through media-***

In India or in U.S Freedom of speech and expression as been of utmost importance. As we all know media plays a very curical role in the lifes of an individual and also for the development and growth of acountry. In a traditional context when we speak about Freedom of Speech it clearly focuses on individual – rights of an individual in particular there right to express their opinion to others. But Freedom of speech is not concentrated individual right to express but at present it involve rights which are associated to newspaper, broadcasting companies and other media corporations, commercial institutions etc. Speeches which are eliminated by mass media are covered under constitutional free speech.

Media provides a wide variety of options to readers, listeners, and viewers with a wide variety of information and in a way it helps or enables the viewers to participate the actively in a democratic country. Media can be considered as the public watchdog. There is also a responsibility on the part of the media to publish true news and together with that there should be protection in a legal framework. When we say protection it does not mean that media are exempted from legal framework.

12 Reno Vs. American Civil Liberties Union, 521 U.S, 844

But at present scenario we can see that there are restrictions on media regulations requiring a newspaper or broadcaster to publish the news, personal attack, foreign affairs would be incompatible with such a right of editorial control. As it is stated that press should provide the eyes are tears of the public. But one of the important question we can see is that who confers the freedom of speech it is the law who media owners or the editorial team owns the freedom of speech.

And there is a recent trend of media raid in India and it has led to the breaking the silence on press freedom. Media and Press are not able to speak. When we do a comparison with U.S we can see that Freedom of Press is given a utmost importance and it is highly protected unlike India. In India as we all know Freedom of Press is done through judiciary. So here we can see a difference between India and U.S And in Hindu Newspaper[13] a article was written on Media raid in BBC Office (Delhi and Bombay). It clearly states that Press Freedom is of Higher importance and judiciary need to revive the doctrine of "effect and consequences" and act without fear and favour.

## Observationsin regard to Freedomof Speech and Expression

The Principle of Declaration- "All people should be afforded equal opportunities to receive, seek and impart information by any means of communication without any discrimination forreasons of race, colour, sex, language, religion political or other opinion". This principle applies to Freedom of expression[14]

Few steps which should be taken for the progressive access are–universal access to infrastructure not only to that but to technology also were large amount of information is available to people across the globe with one click. Elimination of barriers such as the arbitrary barriers which provide hindrance to infrastructure, technology and information which are provided

13 Media Raids and breaking the silence on press freedom.The Hindu, http://www.thehindu.com

14 OAS::Special Rapporteurship for Freedom of Speech and expression, http://www.oas.org

online. And measures to allow a positive enjoyment of right of an individual.

Content Blocking and Filtering all are considered to be the violation of Article -19(1)(a) inIndian Constitution and Article – 13 of American Constitution. Online Privacy, Surveillanceand Freedom of Expression involves two important aspect – First it involves protection of anonymous speech and second it involves protection of the personal data.

## Conclusion

According to the Indian Constitution, everyone has the fundamental right to freedom of speech and expression. The Constitution doesnot, however, enshrine an unqualified individual right to free speech. Instead, it envisions logical limitations that could be imposed on this right by the law.

Numerous laws that impede free speech, such as those that punish sedition, hate speech, or defamation, are legitimated by Article 19 of the Constitution.(2). Through the use of thisclause, it is also possible to inspect movies, books, paintings, etc. Scholars point out that post-independence nation-building and strong national unity were and are historically rooted in the discourse of defending Indian values from foreign forces. Researchers have concluded that any abuse of the law could be harmful. As part of one's larger freedom of speech, which is essential to the operation of a democracy, one has the right to criticize and disagree. Citizens' other civil and political rights are at risk if they are not allowed to freely express themselves.

However, the right to offend is part of the freedom of expression, which is crucial to the functioning of a democracy. Since a little over five years ago, various segments of society have questioned whether "hate speech" can be justified under the right to free speech, with their positions frequently varying from one situation to the next. The functioning of participatory democracy also depends on press freedom.Citizens are unable to participate in a free and fair electoral process without a free press, which limits their ability to make informed decisions.

# The Emerging Technological Advances in a Globalising World – A Threat to Developing Nations

***D. Akshay Kumar[1] & Aparna Ratheesh[2]***

## Abstract

*"Technology is a useful servant but a dangerous master."*

*-Christian Lous Lange*

*Technology has drastically changed how trade is conducted, making it more efficient and cost-effective. Due to technological advancements, businesses have expanded their reach to people and markets. They have reduced trading costs by streamlining processes, improving communication, and accessing market data. The fourth industrial revolution has enabled the automation of tasks through artificial intelligence, offering a range of potential economic and social development benefits in developing countries, such as increased food production. The new technologies may lead to more significant disparities between people in developing countries and between developing and more prosperous regions, creating more significant inequalities than before. The worsening of unemployment,*

1 Research Scholar (JRF); National University of Advance Legal Studies (Nuals) Nad Road, HMT Colony, North Kalamassery, Kerala, 683503, Akshaynuals95@Gmail.com Ph : 8825760024

2 Integrated Ll.m. – Ph.d. Student; National University of Advance Legal Studies (Nuals Nad Road, HMT Colony, North Kalamassery , Kerala , 683503, Aparnaratheesh1999@Gmail.com Ph. 9645074378 , 8129660678

*the amplification of economic power and wealth, and the prevalence of prejudicial algorithms are all interconnected risks that will produce different results and necessitate diverse solutions.*

*Nevertheless, a problem that is shared across all contexts is that too few governments in emerging countries are paying sufficient attention to these issues. The fear that advancing digital technologies will lead to fewer jobs is longstanding, and the idea that new technologies could replace workers is an age-old fear. However, it has been observed that in the past, new technologies have often created more jobs than they have displaced. This time, the new digital technologies are more powerful and far-reaching, and the possibility of new jobs may be limited to increasingly specialized arenas, such as machine learning. The labour cost in emerging markets is substantially lower than in more developed countries, making investing in technologies that replace jobs less costly. However, these countries social and economic environments could be more vulnerable to the potential effects of job- displacing technologies, making the possible consequences more severe.*

*In South Africa, inadequate educational systems and a lack of applicable skills make it difficult for people to secure technology-heavy jobs. Governments are struggling to understand the implications of new technologies and business models, like Uber, which is likely to be used by wealthy elites, further widening the wealth gap and negatively impacting the population. The fourth industrial revolution is being driven by AI algorithms that could be affected by the unconscious biases of those who create them. For example, voice recognition software may have difficulty recognizing different accents. AI can be taught to recognize these accents, but the learning process may be subject to racial and gender prejudices. Therefore the author identifies the issues and proposes reforms to mitigate the AI algorithms, which should be trained and adjusted to different contexts, particularly in developing countries. To promote a more equitable outcome, it is essential to ensure that individuals from developing countries are involved in developing new technological systems.*

**Key Words:** Technological Advancement, Developing Nations, Industrial Revolution, Artificial Intelligence, Machine Learning.

## Introduction

Artificial Intelligence is becoming a more significant aspect of our lives and economy, and major economies like the US and Asia are vying for its advantages. Although it is seen as a driver of productivity and economic

expansion, it may also have a disruptive impact on the economy and society, resulting in the emergence of super companies and a widening of the gap between developed and developing nations. Experts also caution against it because it might lead to more inequality, lower wages, and a smaller tax base. The EU has the opportunity to strengthen its position in the global marketplace and steer AI in a direction that is advantageous to its population and economy. To do this, it must agree on a shared strategy that makes the most of its advantages and permits the most efficient use of the resources of the Member States. There is no agreement on whether and how much the associated hazards will manifest themselves, but wisely crafted legislation might promote the advancement of AI while tempering the negative repercussions.

## What Affects Politicians and Other Elites from Technological Change?

The information and technology revolution is encouraging a more decentralized developmental strategy, linking people more readily, opening up new avenues for personal expression and empowerment, and lowering the likelihood of corruption and the wrongful use of administrative authority. Different governments have reacted to this in various ways. For instance, Bangalore, India, which was included in Newsweek's list of the hottest high-tech towns, has responded in a variety of ways[3]. Through collaborative initiatives with foreign-owned businesses, such as SABC Communications, which recently donated a communications tower in Khayelitsha Township to give residents of that underprivileged community a link to schools, libraries, and other information sources, South Africa is promoting the expansion of opportunity through access to new technologies[4]. There is a

3 Steven Levy, The Hot New Tech Cities, NEWSWEEK, Nov. 9, 1998, available at 1998 WL 17010696.

4 Speech by Minister of Posts, Telecommunications, and Broadcasting to the National Assembly on the Occasion of the Budget Vote for the Department of Communications, May 13, 1998 (visited July 8, 1999).

"social compact" that promotes greater openness in important commercial hubs despite Chinese government authorities' attempts to censor access to the Internet and other cutting- edge communications technologies. Some government officials might believe that promoting information technology has the same short-term benefits and profile as a significant infrastructure project, but more creative and visionary officials might believe that embracing technology can help increase public support as more people come to feel like a part of the developing new economy.

## What Does the Impact of Technology Have on Businesses and their Employees?

Because it has the initiative and entrepreneurial spirit to lead the process of responding to technological changes and discovering ways to benefit from them, the private sector is best positioned to establish the best methods for employing new technology. Three instances show the strength of the new digital "marketplace" and how it affects people who were previously limited to conducting business exclusively with a small number of local clients. In a recent letter to President Clinton, Helen Mutono, a Ugandan lady who sells handcrafted baskets online, said that e-commerce is the only way she will be able to sell her wares on the world market[5]. The three "grassroots" examples of successful Internet use in developing countries are the most crucial information in this text. These examples include the Peruvian agricultural community and the Moroccan women's rug weavers who are now selling their products online, which has a significant impact on their bottom line. New online rivalry, however, has caused upheaval for other firms, particularly smaller ones. Government and corporate leaders recognize that new technologies place a higher value on people who have

5 Clinton Promotes Cyber-Shopping, Urges Industry to Ensure Security, Fraud Protection, NEWSDAY, Dec. 1, 1998, at A51. See also PEOPLink: AIDS Victims Fund: Ugandan Tragedy Brings Blues, But Sapphire Women Conquer (visited July 8, 1999). Dec. 1, 1998, at A51. See also PEOPLink: AIDS Victims Fund: Ugandan Tragedy Brings Blues, But Sapphire Women Conquer (visited July 8, 1999).

the necessary education and abilities and that developing nations are looking for more from the technological revolution than individual success tales of greater sales through the Internet. As a result, emerging nations encounter difficulties integrating new technology and creating a knowledge base, particularly in cases where their talent pool has been depleted by years of "brain drain" and the departure of the most educated residents in search of better prospects overseas. These nations require more skilled professionals to stay and contribute to the development of better training and educational institutions.

## The Potential of AI for Business

Accenture estimates that by 2035, AI may quadruple yearly global economic growth rates, demonstrating the huge economic effect of this technology. According to PwC, the global GDP might rise by up to 14% by 2030 as a result of the rapid development and use of AI. Standardization, automation, and more personalization of goods and services will all benefit from AI. Due to their enhanced AI readiness, quick data acquisition, and improved consumer understanding, North America and China are predicted to benefit most from AI technology. While poorer nations are anticipated to see more moderate growth due to lower rates of adoption of AI technology, Europe will also see major economic advantages from AI[6]. According to the McKinsey Global Institute, by 2030, over 70% of businesses will have adopted at least one sort of AI technology, adding US$13 trillion to the economy. AI is expected to provide a shock to the labour market, resulting in expenses to manage changes in the labour market as well as unfavourable externalities like a reduction in domestic consumption owing to

6 Austria, Belgium, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Ireland, Latvia, Lithuania, Luxembourg, the Netherlands, Poland, Sweden, the United Kingdom, Switzerland, and Norway are included in the PwC paper's definition of "northern Europe". Cyprus, Greece, Hungary, Italy, Malta, Portugal,Slovakia, Slovenia, Spain, Bulgaria, Croatia, Romania, Albania, Belarus, Ukraine, the remaining EFTA nations, and the remainder of eastern Europe are all included in the term "Southern Europe".

unemployment[7]. According to a 2016 Analysis Group report, AI will positively impact jobs, productivity, and GDP in both direct and indirect ways. AI will only have a little effect on growth, as shown by the fact that industries with the highest rates of productivity growth have seen a reduction in their overall economic share. Despite advancements, certain economic sectors will continue to be crucial yet difficult to develop, restricting human labour and inhibiting further innovation.

## Affects Manufacturing

With the help of technologies like the Internet of Things, 5G, cloud computing, big data analytics, smart sensors, augmented reality, 3D printing, and robots, AI is one of the pillars of the digitalization of industry. It may be used for the majority of industrial tasks, from improving industrial research to optimizing multi-machine systems. Supply chains would be built on these benefits, and AI is anticipated to increase the industrial sector's competitiveness through efficiency and productivity increases made possible by data analysis. Additionally, it would increase automation, guarantee more stringent quality control of goods and services, and enable proactive machinery status diagnostics. As Industry 4.0 involves the fusion of several technologies, it could not be realized until the middle of the following decade[8]. The export-led growth model of developing nations may be negatively impacted by AI and automation in wealthy nations, but emerging countries may be able to offset this by utilizing AI in a variety of industries. AI solutions are being sold in international markets by technology companies from developing nations like Brazil, China, Nigeria, and Russia, which may

7 Notes from the AI Frontier: Modeling the impact of AI on the World Economy (no date) McKinsey & Company. Available at: https://www.mckinsey.com/featured-insights/artificial-intelligence/notes-from-the-AI- frontier-modeling-the-impact-of-ai-on-the-world-economy (Accessed: February 16, 2023).

8 Industrial Artificial Intelligence for Industry 4.0-based manufacturing ... (no date). Available at: https://www.researchgate.net/publication/327557176_Industrial_Artificial_Intelligence_for_Industry_40- based_Manufacturing_Systems (Accessed: February 16, 2023).

affect the competitive environment for AI globally. AI is a new element of production that replicates labor tasks at a larger scale and speed, functioning as a new workforce. Brazil's gross value added (GVA) in 2035 will be US$3452 billion without AI and US$3526 billion when AI is seen as a component of production, according to an estimate by Accenture using case studies of Latin American nations to demonstrate the influence of AI.[9]

## Impacts on Businesses, Sectors, and Nations

According to McKinsey, the growth of hugely expanded organizations and a barbell-shaped economy may be caused by AI and automation. This might result in more businesses entering markets outside of their core competencies, more rivalry, and a widening gap between industries with advanced technology and those that lag. Slow or non-adopters will see economic deterioration, whereas early adopters would profit disproportionately. With the help of AI and other technological advancements, leaders may be able to separate themselves from the competition and achieve the highest levels of productivity. Why non- rival innovations are not disseminated to all businesses, favoring global frontier enterprises over laggards, has been questioned by the OECD[10]. In industries including marketing and sales, supply chain management, logistics, and manufacturing, AI is having a big influence and has a lot of economic potentials. According to a 2018 report by the Boston Consulting Group, the transportation, logistics, automotive, and technology industries are leading the way in implementing AI. By 2030, PwC projects that every economic sector will grow by at least 10%, with the services sector growing at the fastest rate (21 percent). Different countries are now adopting AI at different rates, which

9 (https://www.accenture.com/_acnmedia/pdf-48/accenture-ai-southamerica.pdfla=es-la).

10 Andrews, D., Criscuolo, C. and Gal, P.N. (2015) Frontier firms, technology diffusion and public policy, OECD iLibrary. OECD. Available at: https://www.oecd-ilibrary.org/economics/frontier-firms-technology-diffusion-and-public-policy_5jrql2q2jj7b-en (Accessed: February 16, 2023).

raises the possibility that the gap between developed and developing nations could expand. This may result in a slowdown in overall productivity growth and a discussion about the uneven distribution of AI's advantages. High salaries in rich economies provide a bigger incentive to replace human labour with AI than do low wages elsewhere, making it feasible for certain firms to re-source output from less developed nations[11].

## AI's Implications on Labour Markets and Income Distribution

There will be employment creation and job destruction if automation, robots, and AI are broadly used throughout the economy. According to Bruegel, computerization might happen to up to 54% of occupations in the EU during the next 20 years. Job polarization is likely, with higher-paying skilled positions in greater demand and lower-paying jobs being displaced by AI and automation[12]. With increasingly frequent job changes and an increase in contract work, self-employment, and insecure work, labour relations may shift. AI's disruptive impacts may significantly affect income inequality, wages, and income distribution. High-skilled individuals may see an increase in pay due to growing demand, whereas many others may experience wage stagnation or unemployment[13]. Because high- skill employees are more productive and able to perform more tasks, this may have an impact on mid-skilled workers' earnings. AI may result in a "paradox of plenty" yet for many people, groups, and places, technological advancement may simply exacerbate existing disparities. Sensor-motor skills are anticipated to be replaced by AI in non-standard and non- routine

11 McKinsey estimates that leading AI countries could capture an additional 20-25 % in net economic benefits compared with today while developing countries could capture only about 5-15 %. China is an important exception.

12 There are numerous factors at play that render the making of forecasts of the final effect a challenging task. For example, AI diffusion may be slow, which will limit its impact on employment. On the other hand, AI can result in product innovations that foster growth in demand, thereby creating new jobs.

13 In 31 OECD countries, 14 % of jobs are at high risk of automation, while a further 32 % will change significantly.

employment, however, it is unclear how this will affect inequality. While high-skill automation lowers pay disparity, low-skill automation raises it.

## Steps and Safeguards for AI for Development

In this part, guiding ideas are put forward for developing a strong AI ecosystem in India. AI requires access to pertinent data in the digital space, such as free public datasets and 5-star data pipelines. The government's "Digital India" and "Open Government Data" efforts are positive starts in the right direction, and crowdsourcing and AI tools like computer vision might be used to jumpstart the process of generating these types of data sets. It is crucial to teach a larger segment of the public, particularly women, linguistic minorities, and rural areas, to design and manage AI systems for their purposes. The creation of AI frameworks, standards, and APIs can benefit from the open-source movement, which has been successful in India. The idea put up by Jain in 2002 to replace the Gandhian, bottom-up paradigm of information creation and distribution with the Nehruvian top-down one is particularly pertinent to the development of the AI knowledge network. India has a well-established educational system and a skilled labour population, but the country cannot match the need for AI with its current knowledge and skill base. Flagship projects like Deepmind's Alpha Go program can encourage young people to seek jobs in artificial intelligence[14]. Industry, particularly startups, will be crucial in recognizing and realizing the advantages of AI across many industries. India will also need to develop regulatory frameworks that handle issues like safety and quality standards, data security, privacy, and liability, as well as ethical review committees. AI has the potential to revolutionize the fields of healthcare, education, food security, and crisis management, but it also has concerns that must be

14 David Silver, Aja Huang, Chris J. Maddison, Arthur Guez, Laurent Sifre, George van den Driessche, Julian Schrittwieser, Ioannis Antonoglou, Vedavyas Panneershelvam, Marc Lanctot, Sander Dieleman, Dominik Grewe, John Nham, Nal Kalchbrenner, Ilya Sutskever, Timothy P. Lillicrap, Madeleine Leach, Koray Kavukcuoglu, Thore Graepel, and Demis Hassabis. 2016. Mastering the game of Go with deep neural networks and tree search. Nature 529, 7587 (2016), 484–489.

addressed by well- crafted laws and regulations[15]. Human rights, data privacy, and accessibility should all be emphasized in AI policies, with a specific emphasis on vulnerable populations. The importance of e-participation should be emphasized to improve digital literacy.

## Ai-Centric Approach's Risks

Although AI-driven progress has fostered an atmosphere of hope and optimism, it is crucial to foresee and mitigate any possible hazards. The key issues raised by India's socioeconomic setting are covered in this section[16], including worker displacement and the reinforcement of social prejudice. According to McKinsey & Company (2014), improvements in machine learning and natural language interfaces may have an impact on 6– 8 million employees (speech recognition). This might affect the financial security of many others who may be dependent on these wage workers, which would be a significant result for a middle-income country striving to lift many of its residents out of poverty. Concerns about AI's data-driven algorithms picking up biases from the data they are fed are also rising. Caste-based discrimination in call centres was documented by Banerjee et al. (2009). In 2017[17], it is anticipated that there will be 420 million Internet users in India and 300 million mobile Internet users. Particularly in rural India, mobile phones are the main access point to the Internet. Because of the lopsided gender ratios in India's software sector, there is a chance that AI will be slanted strongly toward men. Private firms may prioritize profits over the interests of the less profitable because of the high expenses of creating AI-based applications, which might have long-term effects. There is a chance that the poor will become even more marginalized since it is doubtful that

15 ITU News (2018). "How to govern AI to make it a force for good: Harvard's Urs Gasser", https://news.itu.int/artificial-intelligence-govern-gasser/

16 Erik Brynjolfsson and Andrew McAfee. 2016. The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies. W. W. Norton & Company.

17 IAMAI and Kantar IMRB. 2017. Internet in India – 2016. (2017). Accessed October 26, 2017, bestmediainfo.com/wp-content/uploads/2017/03/Internet-inIndia-2016.pdf.

Google would give its Tamil–Hindi translation engine the same priority as its English–Mandarin engine.

## AI's Effects on Employment and occupations in ohe Public Sector

By improving human-machine interaction in the workplace, particularly in knowledge- intensive jobs, AI increases productivity. Governments must retrain their workforces and invest in them to prevent artificial intelligence (AI) from fostering unemployment. Low- income occupations have an 83 percent likelihood of being automated and replaced by robots. The use of AI in the public sector can result in a more decentralized and interconnected workplace, but Tinholt's research asks whether computers will be able to overcome prejudices and exercise impartial judgment given the facts used to support judgments[18]. AI has the potential to improve work-life balance while reducing regular jobs and activities. It may also make it easier for those with impairments to get employment and enable older workers to stay in the workforce for longer. The use of AI in the workplace of the future, however, necessitates adaptable laws and rules, a social code of ethics[19], and a developing skill set for the workforce to comprehend the many uses and potentials of AI technology.

## What Effects Will AI have on the Workforce?

According to UNDESA research on the effects of the technological revolution on labour markets and income distribution, economic development has been primarily driven by technical advancement, which has increased productivity and reduced costs. However, there is increasing worry about how new technologies, like machine learning and AI, will affect

18 Tinholt, D. (2017) "Unleashing the potential of Artificial Intelligence in the Public Sector", p. 6.

19 British Medical Acupuncture Society (2017). White Paper Work 4.0. Available at: https://www.bmas.de/SharedDocs/Downloads/EN/PDF-Publikationen/a883-whitepaper.pdf;jsessionid=F98FFC003BF1E0911FCEA2AA7227E9ED?blob=publicationF ile&v=3

society and whether this would result in widespread unemployment. A wide range of sectors may require people to have increased digital capabilities as a result of emerging technology. According to UNDESA research on the effects of the technological revolution on labour markets and income distribution, economic development has been primarily driven by technical advancement, which has increased productivity and reduced costs[20]. However, there is increasing worry about how new technologies, like machine learning and AI, will affect society and whether this would result in widespread unemployment. A wide range of sectors may require people to have increased digital capabilities as a result of emerging technology.

## Barriers Facing Developing Countries in the Development of AI

The development of AI in developing nations is hampered by several issues, including a lack of datasets and data of dubious quality. As a result, many ICT initiatives aimed at the poor have been unable to deliver on their promises. The "Index-based" crop insurance plans are an illustration of this; these programs use satellite photos to identify extreme weather, but they are unable to estimate local rainfall properly. Due to agricultural losses brought on by microclimates, several farmers have stopped using their insurance plans. At several stages, from data collecting to actual AI application, the consequences of AI on developing countries are being taken into consideration[21]. In emerging nations including Serbia, Turkey, Russia, Ukraine, Azerbaijan, Angola, Laos, Kazakhstan, Kenya, Uganda, Ecuador, Bolivia, and Peru, China has supplied AI and face recognition software. A face recognition tool is being created by Cloud Walk[22] in collaboration with

20 IResearch (2018). "The development of artificial intelligence in China", https://www.sohu.com/a/227319869_297710.

21 Njagi, K. (2019) Kenyan farmers snap crops with phones to improve insurance payouts, Reuters. Thomson Reuters. Available at: https://www.reuters.com/article/us-climate-change-kenya-insurance/kenyan-farmers- snap-crops-with-phones-to-improve-insurance-payouts-idUSKBN1WQ0Q7 (Accessed: February 17, 2023).

22 "Exporting repression? China's artificial intelligence push into Africa," Council

the Zimbabwean government, but the use of Chinese- produced technology in nations with a patchy record on human rights raises some questions. Face recognition technology is also sold by foreign businesses in South Africa and Kenya, however, it frequently performs badly and is not very useful. A lack of supporting regulatory and policy settings, as well as a history of interrupting Internet access to address issues like exam-cheating and political upheaval, contribute to the low accuracy and precision of African[23] systems. In January 2019 Zimbabwe cut down Internet access for a week owing to instability in disputed elections, while Ethiopia shut down the Internet for three days in June 2019 due to national exams.

***What Can More Economically Advanced Countries Do to Help?***

Given the rising significance of knowledge and information to their economic development, developing nations must reassess their policies and initiatives. Through a range of initiatives, including expanded commercial law development, intellectual property protection, and standards-setting procedures, the Commerce Department and other government agencies are poised to assist developing countries in responding to technological change. Additionally, additional funding is proposed in the President's FY 2000 budget to bolster their judicial and regulatory frameworks[24]. The "Wire the World" program, run by the Geneva-based World Intellectual Property Organization, aims to use new telecommunications and information technologies to connect patent offices through a secure network, streamlining the patent examination procedure and preventing the wastage of limited government resources and duplication of effort. With the use of public-

Foreign Relations, Dec.2018. [Online]. Available: https://www.cfr.org/blog/exporting-repressionchinas-artificial-intelligence-push- africa.

23 J. Snow, "How Africa is seizing an AI opportunity," Fast Company, Mar.2019. [Online]. Available: https://www.fastcompany.com/90308114/how-africa-is-seizing-an-ai-opportunity.

24 Budget of the United States Government, Fiscal Year 2000 § 14, INT'L AFF., at 173-76.

private partnerships, USAID's Leland Initiative for Africa hopes to increase access to the Internet and other telecommunications services in rural regions[25]. Although we may assist developing nations in adjusting to technological change, leaders must ultimately take the initiative.

***What Is the Impact of Technological Change on Developing Countries?***

Both the good and negative effects of new technology may be felt by society. An illustration of how cutting-edge information technology may support and promote indigenous cultures is PEOP Link. It makes use of the Internet to promote regional cultures to a global audience while giving artisans and craftspeople in developing nations a platform to sell their wares. Electronic communication is altering social interaction and has the potential to increase economic disparities rather than narrow them[26]. For those in a position to benefit, technology opens up new opportunities, but it also runs the danger of expanding the divide between those who have and those who do not in a particular society. This is because people are worried that technology will replace labour in some industries, drive more people off the employment market, and not be embraced by business and political elites[27]. A constantly evolving knowledge frontier that threatens to widen disparities is also being created by the explosive rise of technology and the quick expansion of global knowledge, which will put impoverished nations even further behind affluent ones. Although there are no simple answers to these problems, the success stories mentioned below show that information technology may have positive effects on developing nations.

25 USAID Leland Initiative: African Global Information Infrastructure Project .

26 Moppenneer (2020) The impact of digital technology on Indigenous Peoples, The Ethnos Project. Available at: https://www.ethnosproject.org/the-impact-of-digital-technology-on-indigenous-peoples/ (Accessed: February 17, 2023).

27 Dahlman, C.J. (no date) World development report 1998/1999 : Knowledge for development, World Bank. Available at: https://documents.worldbank.org/en/publication/documents reports/documentdetail/729771468328524815/world-development-report-1998-1999-knowledge-for- development (Accessed: February 17, 2023).

## Conclusion

Artificial intelligence and its applications in the public sector for public goods are being actively discussed and collaborated on through the United Nations system and other international and regional efforts. However, the use of AI in the public sector presents a variety of problems for decision-makers. The combined economic, sociological, legal, and ethical implications on society must be taken into account by policymakers as they create sustainable solutions to issues like digital divides, the effects of automation, and the displacement of human labour by robots. Building capacity is crucial to ensuring adequate AI technology deployments and efficient governance to set up an AI-enabled public sector.


JUSTICE
FOR ALL