



AMITY UNIVERSITY

— R A J A S T H A N —

AMITY LAW SCHOOL (ALS)

LL.M Criminal Law

List of students undertaking field project or research projects or internships.

Program Code	Programme name	Name of the students
121045	LLM(Criminal Law)	Aditya Karwasra
121045	LLM(Criminal Law)	Ajeet Kumar
121045	LLM(Criminal Law)	Akanksha Sharma
121045	LLM(Criminal Law)	Anmol Saluja
121045	LLM(Criminal Law)	Asmita Vadnere
121045	LLM(Criminal Law)	Bhadra Singhvi
121045	LLM(Criminal Law)	Bijjoyini Ghosh
121045	LLM(Criminal Law)	Damini Kayathwal
121045	LLM(Criminal Law)	Eesha Sharma
121045	LLM(Criminal Law)	Harish Khan
121045	LLM(Criminal Law)	Isha
121045	LLM(Criminal Law)	Jahnvi Sen
121045	LLM(Criminal Law)	Mohit Garg
121045	LLM(Criminal Law)	Naval Darshna Ravindra
121045	LLM(Criminal Law)	Nikita Indrasingh Purohit
121045	LLM(Criminal Law)	Pratistha Jain
121045	LLM(Criminal Law)	Qurait Ul Ain
121045	LLM(Criminal Law)	Rahul Sharma
121045	LLM(Criminal Law)	Rajarshi Mehta
121045	LLM(Criminal Law)	Rajat Singhal
121045	LLM(Criminal Law)	Shashwat Dhankhar
121045	LLM(Criminal Law)	Surendra Sangwa
121045	LLM(Criminal Law)	Urooj Amin
121045	LLM(Criminal Law)	Uttam Singh Ranwa
121045	LLM(Criminal Law)	Varsha Singh Choudhary
121045	LLM(Criminal Law)	Vikash Chaudhari
121045	LLM(Criminal Law)	Yashpal Singh Rathore
121045	LLM(Criminal Law)	Zarka

“Right to die with dignity: Euthanasia and the Indian Law”??

Dissertation Submitted in Partial Fulfillment
of the Academic Requirement of Degree of **Master of Laws**
(LL.M) in (Criminal Law)



At
AMITY LAW SCHOOL
AMITY UNIVERSITY RAJASTHAN
JAIPUR

SUBMITTED BY:

Aditya Karwasra

LLM 2nd SEMESTER

(CRIMINAL LAW)

A215104520028

2020-2021

SUPERVISED BY:

Mr. Vedansh Sharma

ASSISTANT PROFESSOR

AMITY LAW SCHOOL

DECLARATION

I **Aditya Karwasra** bearing enrolment no. **A215104520028**, **2nd Semester**, pursuing **LL.M in Criminal Law** at **Amity Law School, Amity University Rajasthan, Jaipur**, do hereby, declare that the work presented in this thesis entitled **“RIGHT TO DIE WITH DIGNITY: EUTHANASIA AND THE INDIAN LAW”** is conducted under the supervision of **Mr. Vedansh Sharma (Asst. Professor of Law- Amity Law School)**, which is submitted for the award of degree of **LL.M in Amity Law School**, is my original work and has not been submitted by me in any other university for degree or diploma.

Place:

Date:

Aditya Karwasra

CERTIFICATE

This is to certify that **Ms. Aditya Karwasra** student of **LL.M (Criminal Law)** has completed her dissertation, to be submitted in partial fulfilment of the requirement for the degree of Master of Laws bearing the title **“Right to die with dignity: Euthanasia and the Indian Law”?** It is further certified that this work is the result of her own efforts and is fit for evaluation.

Aditya karwasra

LL.M 2nd Semester

(Criminal Law)

2020- 2021

A2151204520028

Mr. Vedansh Sharma

Assistant Professor

Amity Law School

**JUDICIAL CONTROL OF ADMINISTRATIVE
DISCRETION IN INDIA: A STUDY**

**Dissertation Submitted in Partial Fulfilment of the Academic
Requirement of Degree of Master of Laws (LL.M) in (Criminal Law)**

At
Amity University

SUBMITTED BY

**AJEET KUMAR
A215104520021**

UNDER THE SUPERVISION OF

**Ms. Sonali Bhatnagar
Ass. Professor Law**



**Amity University
SP-1 Kant Kalwar, NH11C
RIICO Industrial Area, Jaipur
Rajasthan-303007**

DECLARATION

I Ajeet Kumar, student of Master of Laws (Criminal Law), hereby declare that the dissertation titled “JUDICIAL CONTROL OF ADMINISTRATIVE DISCRETION IN INDIA: A STUDY” which is submitted by me to Amity Law School, Jaipur, Rajasthan in partial fulfilment of the requirement for the award of the degree of Master of Laws (LLM) by the Amity University, Jaipur, Rajasthan is my original work. It is further declared that all the sources of information used in the dissertation have been duly acknowledged. I understand that dissertation may be electronically checked for plagiarism by the use of plagiarism detection software to assess the originality of the submitted work.

Place:

Date:

Signature

CERTIFICATE

On the basis of declaration submitted by Ajeet Kumar, student of Master of Laws (Criminal Law), I hereby certify that the dissertation titled “JUDICIAL CONTROL OF ADMINISTRATIVE DISCRETION IN INDIA: A STUDY” which is submitted by to Amity Law School, Jaipur, Rajasthan in partial fulfilment of the requirement for the award of the degree of Master of Laws (LLM) by the Amity University, Jaipur, Rajasthan has been carried out by him under my guidance and supervision.

Signature Supervisor

**A Critical Overview of The Rights of Arrested and Detained Persons in the Indian
Criminal Justice System**

Dissertation Submitted in Partial Fulfillment of the Academic Requirement for the
Award of Degree of **Master of Laws**

(LL.M.) in (Criminal Law)

At

**AMITY LAW SCHOOL AMITY
UNIVERSITY, RAJASTHAN**

JAIPUR

BATCH

2020-2021



SUBMITTED BY:

AKANKSHA SHARMA

LL.M. (CRIMINAL LAW)

A215104520018

2nd SEMESTER

SUBMITTED TO:

DR. VINOD KUMAR

ASSOCIATE PROFESSOR

AMITY LAW SCHOOL

DECLARATION

I, **AKANKSHA SHARMA** student of **LL.M. (Criminal Law) 2nd Semester**, Enrollment No. **A215104520018**, declare that this Dissertation and the work presented in it is original and has been generated by me as the result of my own original research.

A CRITICAL OVERVIEW OF THE RIGHTS OF AND DETAINED PERSONS IN THE INDIAN CRIMINAL JUSTICE SYSTEM

I confirm that:

- This work was done wholly or mainly while in candidature for a professional degree at this college;
- Where any part of this dissertation has previously been submitted for a degree or any other qualification at this University or any other institution; this has been clearly stated;
- Where I have consulted the published work of others, this is always clearly attributed;
- Where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my own work;
- I have acknowledged all main sources of help;
- Where the thesis is based on work done by myself jointly with others; I have made clear exactly what was done by others and what I have contributed myself.

AKANKSHA SHARMA
LL.M. (Criminal Law)
AMITY LAW SCHOOL
DATED: 10.05.2021



AMITY UNIVERSITY — JAIPUR —

CERTIFICATE

This is to certify that the Dissertation entitled **A CRITICAL OVERVIEW OF THE RIGHTS OF AND DETAINED PERSONS IN THE INDIAN CRIMINAL JUSTICE SYSTEM** is a bonafide record of independent research work done by **AKANKSHA SHARMA** (Enrollment No. **A215104520008**) under my supervision and submitted to **Amity Law School** in partial fulfillment of the Academic Requirement for the award of the Degree of **Master of Laws (LL.M.) in (Criminal Law)** At **AMITY LAW SCHOOL, AMITY UNIVERSITY RAJASTHAN, JAIPUR.**

Further certify that work is perfect for submission and evaluation.

I wish him all the success in life.

Dr. Vinod Kumar
Associate Professor
AMITY LAW SCHOOL

SEXUAL HARRASMENT OF WOMEN:
Studying Male Behaviour and Their Proclivities

Dissertation Submitted in Partial Fulfillment of the Academic
Requirement of Degree of **Master of laws (LL.M)** in
(Criminal Law)

At

Amity University Rajasthan

SUBMITTED BY: ANMOL SALUJA
ENROLLMENT NUMBER: A215104520014

UNDER THE SUPERVISION OF:
DR. ABHISHEK BAPLAWAT



DECLARATION

I declare that the dissertation entitled '**Sexual harassment of women: *Studying Male Behaviour and Their Proclivities***' is the outcome of my own research conducted under the supervision of Dr. Abhishek Baplawat (Assistant Professor) Amity Law School, Jaipur.

I further declare that to the best of my knowledge the dissertation does not contain any part of any work which has been submitted for the award of any degree either in this university or any other university.

Further whenever any book, article, research work or any other work has been used to carry out this study, the same has been fully and properly cited and acknowledged.

PLACE: Jodhpur

STUDENT NAME: Anmol Saluja

Date: 10/05/2021

Enrollment No. - A215104520014

Assistant Professor Dr. Abhishek Baplawat
Amity University, Jaipur

CERTIFICATE

This is to certify that the research work entitled '**Sexual harassment of women: *Studying Male Behaviour and Their Proclivities***' has been done by **Ms. Anmol Saluja**, Enrollment no. A215104520014 , under my supervision in partial fulfillment of the requirement for the award of degree of Masters of Law of Amity University, Jaipur.

Further certify that work is fit for submission and evolution.

I wish her all the success in life.

(Dr. Abhishek Baplawat)

**“CRIME AGAINST WOMEN IN INDIA : ISSUES AND
CHALLENGES”**

**Dissertation Submitted in Partial Fulfillment
Of the Academic Requirement of Degree of Master of Laws
(LL.M) in (Criminal Law)**

At

**AMITY LAW SCHOOL
AMITY UNIVERSITY RAJASTHAN
JAIPUR**



**SUBMITTED BY
ASMITA VADNERE
LLM 2 ND SEMESTER
CRIMINAL LAW
2020-2021**

**SUPERVISIED BY:
Ms. SONALI BHATNAGAR
ASSISTANT PROFESSOR
AMITY LAW SCHOOL**

DECLARATION

I, **ASMITA VADNERE** student of **LL.M. (Criminal Law) 2nd Semester**, Enrolment No. **A215104520019**, declare that this Dissertation and the work presented in it is original and has been generated by me as the result of my own original research.

“CRIME AGAINST WOMEN IN INDIA : ISSUES AND CHALLENGES”

I confirm that:

- This work was done wholly or mainly while in candidature for a professional degree at this college;
- Where any part of this dissertation has previously been submitted for a degree or any other qualification at this University or any other institution; this has been clearly stated;
- Where I have consulted the published work of others, this is always clearly attributed;
- Where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my own work;
- I have acknowledged all main sources of help;
- Where the thesis is based on work done by myself jointly with others; I have made clear exactly what was done by others and what I have contributed myself.

ASMITA VADNERE

LL.M. (Criminal Law)

AMITY LAW SCHOOL

DATED: 28.04.2021

CERTIFICATE

This is to certify that the Dissertation entitled “**CRIME AGAINST WOMEN IN INDIA : ISSUES AND CHALLENGES**” is a bonafide record of independent research work done by ASMITA VADNERE (Enrolment No. A215104520019) under my supervision and submitted to Amity Law School in partial fulfilment of the Academic Requirement for the award of the Degree of Master of Laws (LL.M.) in (Criminal Law) At AMITY LAW SCHOOL, AMITY UNIVERSITY RAJASTHAN, JAIPUR.

Further certify that work is perfect for submission and evaluation.

I wish him all the success in life.

Ms. Sonali Bhatnagar

Assistant Professor

AMITY LAW SCHOOL

A Socio-Legal Study of Crimes against Children in India

Dissertation Submitted in Partial Fulfilment
Of the Academic Requirement of Degree of **Master of Laws**
(LL.M) in (Criminal Law)

At

AMITY LAW SCHOOL
AMITY UNIVERSITY RAJASTHAN
JAIPUR



SUBMITTED BY:

BHADRA SINGHVI

LLM 2nd SEMESTER

(CRIMINAL LAW)

2020-2021

SUPERVISED BY:

DR. VINOD KUMAR

ASSOCIATE PROFESSOR

AMITY LAW SCHOOL

Student declaration

I Bhadra Singhvi, student of LLM Criminal law at Amity Law School, Jaipur declare that the dissertation has been composed by me and that the work has not been submitted for any other degree or professional qualification. I confirm that the work submitted is my own, except where work which has formed part of jointly-authored publications has been included. My contribution and those of the other authors to this work have been explicitly indicated below. I confirm that appropriate credit has been given within this dissertation where reference has been made to the work of others.

Signature:

Name: Bhadra Singhvi

Date: 10th May 2021

Certificate

This is to certify that, the dissertation entitled “*A SOCIO-LEGAL STUDY OF CRIME AGAINST CHILDREN IN INDIA*” is the bonafide work done by Ms. Bhadra Singhvi during his Masters in Law course 2020-2021, done under my supervision and is submitted in partial fulfillment for the requirement of the Post graduation course at Amity Law School, Jaipur.

Dr Vinod Kumar

Associate professor

Amity Law School Jaipur

SEXUAL HARASSMENT AT WORKPLACE: #METOO MOVEMENT AND ITS IMPACT

Dissertation Submitted in Partial Fulfillment
of the Academic Requirement of Degree of **Master of Laws**
(LL.M) in (Criminal Law)

At

AMITY LAW SCHOOL
AMITY UNIVERSITY RAJASTHAN
JAIPUR



SUBMITTED BY:

BIJOYINI GHOSH

LLM 2nd SEMESTER

A215104520002

(CRIMINAL LAW)

2020-2021

SUPERVISED BY:

DR. VINOD KUMAR

ASSOCIATE PROFESSOR

AMITY LAW SCHOOL



AMITY UNIVERSITY — JAIPUR —

DECLARATION

I, **BIJJOYINI GHOSH** student of **LL.M. (Criminal Law) 2nd Semester**, Enrollment No. **A215104520002**, declare that this Dissertation and the work presented in it is original and has been generated by me as the result of my own original research.

SEXUAL HARASSMENT AT WORKPLACE: #METOO MOVEMENT AND ITS IMPACT

I confirm that:

- This work was done wholly or mainly while in candidature for a professional degree at this college;
- Where any part of this dissertation has previously been submitted for a degree or any other qualification at this University or any other institution; this has been clearly stated;
- Where I have consulted the published work of others, this is always clearly attributed;
- Where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my own work;
- I have acknowledged all main sources of help;
- Where the thesis is based on work done by myself jointly with others; I have made clear exactly what was done by others and what I have contributed myself.

BIJJOYINI GHOSH

LL.M. (Criminal Law)
AMITY LAW SCHOOL
Dated: 10.05.2021

CERTIFICATE

This is to certify that the Dissertation entitled **SEXUAL HARASSMENT AT WORKPLACE: #METOO MOVEMENT AND ITS IMPACT** is a bonafide record of independent research work done by **BIJJOYINI GHOSH** (Enrollment No. **A215104520002**) under my supervision and submitted to **Amity Law School** in partial fulfillment of the Academic Requirement for the award of the Degree of **Master of Laws (LL.M.) in (Criminal Law)** At **AMITY LAW SCHOOL, AMITY UNIVERSITY RAJASTHAN, JAIPUR.**

Further certify that work is perfect for submission and evaluation.

I wish her all the success in life.

Dr. Vinod Kumar
Associate Professor
AMITY LAW SCHOOL

**EXAMINING RELEVANCE AND USE OF SEDITION
LAWS, FREEDOM OF SPEECH AND JUDICIAL
TRENDS**

Dissertation Submitted in Partial Fulfilment of the Academic Requirement of Degree of

LL.M. (Criminal Law)

At

AMITY LAW SCHOOL

AMITY UNIVERSITY RAJASTHAN

JAIPUR



SUBMITTED BY:

DAMINI KAYATHWAL

LLM 2nd SEMESTER

(CRIMINAL LAW)

2020-2021

SUPERVISED BY:

DR. ASHU MAHARSHI

ASSITANT PROFESSOR

AMITY LAW SCHOOL

DECLARATION

I, **DAMINI KAYATHWAL** bearing enrolment no. **A2151104520023**, **2nd Semester**, pursuing **L.L.M in Criminal Law** at Amity Law School, Amity University Rajasthan, Jaipur, do hereby declare that this topic is my original work prepared by me in partial fulfilment of the Academic Requirement of Degree of **Master of Laws (LL.M in Criminal Law)** under the supervision of **Dr. Ashu Maharshi (Asst. Professor of Law- Amity Law School)**.

Neither the said work nor any part thereof, has earlier been submitted to any University or Institution for the award of any degree or diploma. **Further wherever any book, article, research work or any other work has been used to carry out this study, the same has been fully cited and acknowledged.**

CERTIFICATE

This is to certify that Ms. Damini Kayathwal, student of L.L.M (Criminal Law) has completed her dissertation, to be submitted in partial fulfilment of the requirement for the degree of Master of Laws bearing the title “Examining Relevance And Use Of Sedition Laws, Freedom Of Speech And Judicial Trends”. It is further certified that this week work is the result of her own efforts and is fit for evaluation.

DAMINI KAYATHWAL
LLM
(CRIMINAL LAW)
2020-2021

DR. ASHU MAHARSHI
ASSITANT PROFESSOR
AMITY LAW SCHOOL

A Socio-Legal Study of Crimes of Honor against Women in India

Dissertation Submitted in Partial Fulfilment
of the Academic Requirement of Degree of **Master of Laws**
(LL.M) in (Criminal law)

At

AMITY LAW SCHOOL
AMITY UNIVERSITY RAJASTHAN
JAIPUR



SUBMITTED BY:

EESHA SHARMA

LLM 2nd SEMESTER

(CRIMINAL LAW)

2020-2021

SUPERVISED BY:

DR. VINOD KUMAR

ASSOCIATE PROFESSOR

AMITY LAW SCHOOL

DECLARATION

I, Eesha Sharma bearing enrolment no. A215120450009, 2nd Semester, pursuing LL.M in Criminal Law at Amity Law School, Amity University Rajasthan, Jaipur, do hereby declare that this topic is my original work prepared by me in partial fulfilment of the Academic Requirement of Degree of Master of Laws (LL.M in Criminal Law) under the supervision of Professor Vinod Kumar. Neither the said work nor any part thereof, has earlier been submitted to any University or Institution for the award of any degree or diploma. Further wherever any book, article, research work or any other work has been used to carry out this study, the same has been fully cited and acknowledged.

CERTIFICATE

This is to certify Ms Eesha Sharma student of LL.M (Criminal Law) has completed her dissertation, to be submitted in partial fulfilment of the requirement for the degree of Master of Laws bearing the title “A Socio-Legal Study of Crimes of Honour against Women in India”. It is further certified that this work is the result of her own efforts and is fit for evaluation.

Eesha Sharma A215120450009

LLM

CRIMINAL LAW (2020-2021)

Dr. Vinod Kumar

Associate Professor

Amity Law School

**THE SOCIO-LEGAL ASPECT OF
INSTITUTIONAL JUVENILE JUSTICE SYSTEM**

*Dissertation Submitted in Partial Fulfillment of the Academic Requirement of
Degree of Master of Laws (LL.M) in (Criminal law)*

At

AMITY UNIVERSITY

SUBMITTED BY

HARISH KHAN

A215104520001

SUPERVISED BY

Dr. ASHU MAHARSHI



SP-1 Kant Kalwar, NH11C, RIICO Industrial Area, Jaipur, Rajasthan 303007

DECLARATION BY THE CANDIDATE

I hereby declare that the dissertation entitled “**THE SOCIO-LEGAL ASPECT OF INSTITUTIONAL JUVENILE JUSTICE SYSTEM,**” submitted at **AMITY UNIVERSITY, JAIPUR** is the outcome of my own work carried out under the supervision of **Dr. Ashu maharshi**.

I further declare that to the best of my knowledge, the dissertation does not contain any part of work, which has not been submitted for the award of any degree either in this university or in any other institution without proper citation.

HARISH KHAN

A215104520001

AMITY UNIVERSITY

JAIPUR

MAY-10-2021

CERTIFICATE OF SUPERVISOR

This is to certify that the work reported in the LL.M dissertation entitled “**THE SOCIO-LEGAL ASPECT OF INSTITUTIONAL JUVENILE JUSTICE SYSTEM,**” submitted by **Harish khan** at **Amity University, Jaipur** is a bona fide record of his original work carried out under my supervision. To the Best of my knowledge and belief, the dissertation: (i) embodied the work of the candidate himself; (ii) has duly been completed; and (iii) is up to the standard both in respect of contents and language for being referred to the examiner.

Dr. ASHU MAHARSHI
AMITY UNIVERSITY, JAIPUR

JAIPUR
MAY-10-2021

DISSERTATION

FORENSIC EVIDENCE

ISHA

FORENSICS AS A TOOL OF EVIDENCE IN CRIMINAL JUSTICE SYSTEM: A COMPARATIVE STUDY OF U.S., U.K. AND INDIA

Dissertation - Synopsis Submitted in Partial Fulfillment
of the Academic Requirement of Degree of **Master of Laws**

(LL.M) in (Criminal Law)

At

AMITY LAW SCHOOL

AMITY UNIVERSITY RAJASTHAN

JAIPUR



SUBMITTED BY:

ISHA

LLM 2nd SEMESTER

(CRIMINAL LAW)

2020-2021

SUPERVISED BY:

DR. VINOD KUMAR

ASSOCIATE PROFESSOR

AMITY LAW SCHOOL

DISSERTATION

FORENSIC EVIDENCE

ISHA

DECLARATION BY THE CANDIDATE

I, Isha, the undersigned solemnly declare that the dissertation titled (FORENSIC SCIENCE AS EVIDENCE IN THE CRIMINAL JUSTICE SYSTEM-A COMPARATIVE ANALYSIS OF INDIA, US AND UK) is based on my own work carried out during the course of my study under the supervision of Dr. Vinod Kumar.

I assert the statements made and conclusions drawn are an outcome of my research work. I further certify that

I. The work contained in the report is original and has been done by me under the general supervision of my supervisor.

II. The work has not been submitted to any other Institution for any other degree/diploma/certificate in this university or any other University of India or abroad.

III. I have followed the guidelines provided by the university in writing the report.

IV. Whenever I have used materials (data, theoretical analysis, and text) from other sources, I have given due credit to them in the text of the report and giving their details in the references.

Isha

Enrollment No. A215104520025

DISSERTATION

FORENSIC EVIDENCE

ISHA

CERTIFICATE FROM THE SUPERVISOR

This is to certify that the work incorporated in the project report entitled “FORENSIC SCIENCE AS EVIDENCE IN THE CRIMINAL JUSTICE SYSTEM-A COMPARATIVE ANALYSIS OF INDIA, US AND UK” is a record of work carried out by Isha, Enrollment No. A215104520025 under my guidance and supervision for the award of Degree of Master of Laws in Criminal Law at Amity Law School, Amity University Rajasthan, Jaipur.

To the best of my knowledge and belief the dissertation

I. Embodies the work of the candidate herself,

II. Has duly been completed,

III. Fulfils the requirement of the Ordinance relating to the Master degree of the University and

IV. Is up to the desired standard both in respect of contents and language for being referred to the examiners.

DR. VINOD KUMAR

(GUIDE)

(ASSOCIATE PROFESSOR, AMITY LAW SCHOOL, AMITY UNIVERSITY RAJASTHAN, JAIPUR)

The dissertation as mentioned above is here by being recommended and Forwarded for examination and evaluation

Dr. Vinod Kumar

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

Violation of Human Rights of Prisoners- A Critical Analysis

Dissertation Submitted in Partial Fulfillment

Of the Academic Requirement Degree of **Masters of Law**

(LLM) in (Criminal Law)

At

AMITY LAW SCHOOL

AMITY UNIVERSITY RAJASTHAN

JAIPUR



SUBMITTED BY: -

JAHNVI SEN

LLM 2ND SEM

(CRIMINAL LAW)

ENROLMENT NO.- A215104520006

SUPERVISED BY: -

MR. KESHAV JHA SIR

ASSISTANT PROFESSOR

AMITY LAW SCHOOL

CANDIDATE DECLARATION

I, Jahnvi Sen, LLM (Criminal Law) student of Amity Law School, Jaipur, do hereby declare that I have duly worked on my dissertation entitled “*Violation of Human Rights of Prisoners- A Critical Analysis*” under the Supervision of Mr. Keshav Jha Sir, Assistant Professor (Law) ALS, Amity University Rajasthan .

Dated 10th May 2021

SUPERVISOR CERTIFICATE

This is to certify that Ms. Jahnvi Sen who is bonafide student having enrolment no. A215104520006. She is submitting this Dissertation entitled “Violation of Human Rights of Prisoners- A Critical Analysis” for awarding the degree of Masters of Law. She has worked on the topic under my constant supervision and guidance.

Name of the Supervisor: - Mr. Keshav Jha Sir

Designation:- Assistant Professor

ALS, Amity University Rajasthan

ANALYSIS OF WILDLIFE CRIME PROTECTION LAWS IN INDIA: A LESS WALKEN ROAD

Dissertation Submitted in Partial Fulfilment of the Academic Requirement of Degree of

LL.M. (Criminal Law)

At

AMITY LAW SCHOOL

AMITY UNIVERSITY RAJASTHAN

JAIPUR



SUBMITTED BY:

MOHIT GARG

LLM 2nd SEMESTER

(CRIMINAL LAW)

2020-2021

SUPERVISED BY:

MR. PRATEEK DEOL

ASSITANT PROFESSOR

AMITY LAW SCHOOL

DECLARATION

*I, MOHIT GARG bearing enrolment no. A215104520020, 2nd Semester, pursuing LL.M in Criminal Law at Amity Law School, Amity University Rajasthan, Jaipur, do hereby declare that this topic is my original work prepared by me in partial fulfilment of the Academic Requirement of Degree of Master of Laws (LL.M in Corporate Law) under the supervision of **Mr. Prateek Deol (Asst. Professor of Law- Amity Law School)**. Neither the said work nor any part thereof has earlier been submitted to any University or Institution for the award of any degree or diploma. Further wherever any book, article, research work or any other work has been used to carry out this study, the same has been fully cited and acknowledged.*

ACKNOWLEDGEMENT

It is with immense joy and pleasure that I record my deep sense of indebtedness and gratitude to ***Mr. Prateek Deol my esteemed guide***, for his noble guidance and continuous, galvanizing encouragement which has been the source of inspiration and great driving force throughout the span of this work. It was very kind of him to have spent a lot of his valuable time in the supervision of this work. While offering this piece of work ***I obliged my sincere thanks, deep respect and gratitude the Head of institution Prof. Dr. Saroj Bohra.***

I want to take this opportunity also to express my genuine respect and gratefulness to all my other teachers, Amity Law School library, friends and family members, who have helped me in my study.

I express my sincere thanks to Mr. Prateek Deol who took personal pain to help and direct me in collection of study material and prepare this dissertation at appropriate stages.

Thank You.

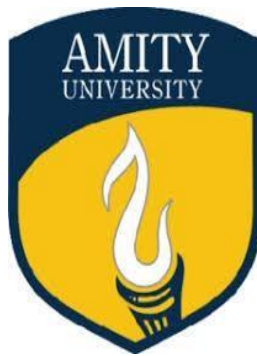
MOHIT GARG LL.M (CRIMINAL LAW)

II SEMESTER A215104520020

2020-2021

PROFILING WHITE COLLAR CRIMES:
A CRITICAL ANALYSIS OF FINANCIAL CRIMES IN INDIA

DISSERTATION SUBMITTED
IN PARTIAL FULFILMENT OF THE ACADEMIC REQUIREMENT OF DEGREE OF
MASTERS OF LAW (LL.M) IN (CRIMINAL LAW)



AT
AMITY LAW SCHOOL
AMITY UNIVERSITY RAJASTHAN
JAIPUR

SUBMITTED BY:

Ms. Darshna Naval

LL.M 2nd Semester

(Criminal Law) Amity Law School

2020-2021

SUPERVISED BY:

Mr. Vedansh Sharm

Assistant Professor

DECLARATION

I, Darshna Naval, bearing enrolment no. A215104520013 2nd Semester, pursuing LL.M in Criminal Law at Amity Law School, Amity University Rajasthan, Jaipur, do hereby declare that this topic is my original work prepared by me in partial fulfilment of the Academic Requirement of Degree of Master of Laws (LL.M in Criminal Law) under the supervision of Mr. Vedansh Sharma (Assistant Professor of Law- Amity Law School). Neither the said work nor any part thereof, has earlier been submitted to any University or Institution for the award of any degree or diploma.

Further wherever any book, article, research work or any other work has been used to carry out this study, the same has been fully cited and acknowledged.

CERTIFICATE

This is to certify that **Ms. Darshna Naval**, student of **LL.M (Criminal Law)** has completed her dissertation, to be submitted in partial fulfilment of the requirement for the degree of Masters of Law bearing the title '**Profiling White Collar Crimes: A Critical Analysis of Financial Crimes in India**'. It is further certified that this work is the result of her own efforts and is fit for evaluation.

Ms. Darshna Naval

LL.M (Criminal Law)

2020-2021

A215104520013

Mr. Vedansh Sharm

Assistant Professor

Amity Law School

“Marital Rape in India and United States: A Comparative Study”

“MARITAL RAPE IN INDIA AND UNITED STATES: A COMPARATIVE STUDY”

Dissertation Submitted in Partial Fulfilment
of the Academic Requirement of Degree of Master of Laws
LL.M in (Criminal law)



At

AMITY LAW SCHOOL

AMITY UNIVERSITY RAJASTHAN

JAIPUR

SUBMITTED BY:

NIKITA PUROHIT

LLM 2ND SEMESTER

(CRIMINAL LAW)

2020-2021

SUPERVISED BY:

PROF. DR. SAROJ BOHRA

DIRECTOR

AMITY LAW SCHOOL

DECLARATION

I, **Nikita Indrasingh Purohit** bearing enrolment no. **A21542620006**, **2nd Semester**, pursuing **LL.M in Criminal Law at Amity Law School, Amity University Rajasthan, Jaipur**, do hereby declare that this topic is my original work prepared by me in partial fulfilment of the Academic Requirement of Degree of **Master of Laws (LL.M in Criminal Law)** under the supervision of Prof. **Dr. Saroj Bohra (Director- Amity Law School)**.

Neither the said work nor any part thereof, has earlier been submitted to any University or Institution for the award of any degree or diploma.

Further wherever any book, article, research work or any other work has been used to carry out this study, the same has been fully cited and acknowledged.

CERTIFICATE

This is to certify that **Ms. Nikita Purohit** student of **LL.M (Criminal Law)** has completed her dissertation, to be submitted in partial fulfilment of the requirement for the degree of Master of Laws bearing the title “**Marital Rape in India and United States: A Comparative Study**”. It is further certified that this work is the result of his own efforts and is fit for evaluation.

Nikita Purohit
LLM (Criminal Law)
2020-2021
A21542620006

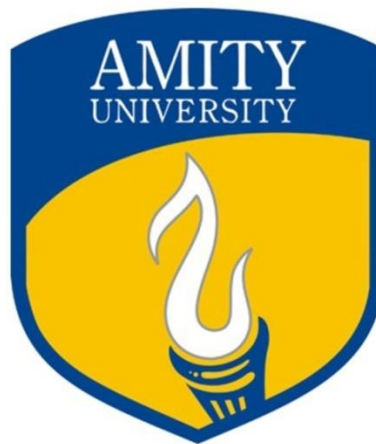
Prof. Dr. Saroj Bohra
Director
Amity Law School

**JUDICIARY AND CRIMINAL STATUTES OF INDIA: A SQUEAKY WHEEL IN THE
HOPE OF GETTING GREASE**

Dissertation submitted in partial fulfillment for the award of degree

OF

LL.M.



AT

AMITY LAW SCHOOL

AMITY UNIVERSITY RAJASTHAN

JAIPUR

SUBMITTED BY

PRATISTHA JAIN

LLM 2ND SEMESTER

(CRIMINAL LAW)

2020-2021

SUPERVISED BY

MR. PRATEEK DEOL

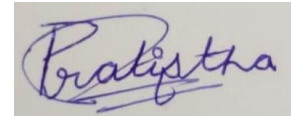
ASSISTANT PROFESSOR

AMITY LAW SCHOOL

CANDIDATE DECLARATION

I hereby declare that the dissertation entitled: **JUDICIARY AND CRIMINAL STATUTES OF INDIA: A SQUEAKY WHEEL IN THE HOPE OF GETTING GREASE** submitted by me to Amity Law School, Rajasthan in partial fulfillment of the requirement for the award of the degree of LL.M in Criminal Law is a record of bona fide dissertation carried out by me under the guidance of Mr. Prateek Deol, Assistant Professor, Amity Law School. I further declare that the work reported in this dissertation has not been submitted anywhere else and will not be submitted either in part or in full, for the award of any other degree or diploma in this institute or any other institute or University.

Signature of the candidate



Pratistha Jain

Enrollment no:

A215104520004

Amity Law School,

Amity University, Rajasthan

Date:

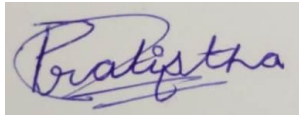
10th May, 2021

SUPERVISOR CERTIFICATE

This is to certify that dissertation work done in the dissertation having title “**JUDICIARY AND CRIMINAL STATUTES OF INDIA: A SQUEAKY WHEEL IN THE HOPE OF GETTING GREASE**”, was carried out by “**Ms. Pratistha Jain**” Enrollment no: **A215104520004** at **Amity Law School**, for the partial fulfillment of **LL.M.** (specialization in Criminal Law) degree to be awarded by Amity University Rajasthan. To the best of my knowledge and belief, the dissertation: (i) embodied the work of the candidate himself; (ii) has duly been completed; and (iii) up to the standard both in respect of contents and language for being referred to the examiner.

This dissertation work has been carried out under my supervision and is to my satisfaction.

Signature of the Student:



Pratistha Jain

Signature of Supervisor:

Mr. Prateek Deol

Assistant Professor

Department-

Amity Law School

Name of University-

Amity University

Date- 10th May, 2021

CHAPTER 1

INTRODUCTION

“To call woman the weaker sex is a libel; it is man’s injustice to woman. If by strength is meant brute strength then indeed is woman less brute than man. If by strength is meant moral power then woman is immeasurably man’s superior. Has she not greater intuition is she not more self-sacrificing, has she not greater powers of endurance has she not greater courage? Without her man could not be. If nonviolence is the law of our being the future is with woman. Who can make a more effective appeal to the heart than woman?”

According to the Rigveda and other scriptures, ancient Indian women held a high position of respect in society. From the Vedic era to modern times, volumes could be written about the role of our women and their heroic deeds. Women lost their status and were relegated to the background as a result of social, political, and economic changes. Many evil rituals and practices arose, enslaving women and binding them to the confines of their homes.¹ According to official figures, women's sex ratio, health status, literacy rate, job participation rate, and political participation rate are all decreasing. On the other hand, in various parts of India, social evils such as dowry deaths, child marriage, domestic abuse, rape, sexual assault, and exploitation of women workers are rampant. Embarrassment, rape, abduction, molestation, dowry death, torture, and wife-beating have all become more common over time.²

Women have always been respected in Indian society. Man and woman represent the two halves of the divine body in Hinduism. There is no difference between them in terms of dominance or inferiority. The super-women of Hindu literature, such as Gargi, Maitreyi, and Sulabha, possessed a thinking faculty much superior to that of ordinary mortals. Saraswati, Durga, Laxmi, Kali, and other female deities are worshipped all over the world. According to the Mahabharat, honoring women is tantamount to worshiping the goddess of wealth. On the other hand, since the time of the Rig Veda, the patriarchal system has persisted. Men created customs and values to benefit men. Women suffer in silence as a result of sexism. Historically, Indian women have been forced to play dual roles. To ensure that women effectively play their

¹ Aruna Goel, Violence and protective measures for women development and empowerment 3-4 (Deep & Deep Publications, New Delhi, 2004).

² Awadesh Kumar Singh & Jayanta Choudhury, Violence against women and children issues and concerns 1 (Serials Publications, New Delhi, 2012).

traditional roles of nurturing as daughters, mothers, husbands, and daughters-in-law, the power of a woman is evoked. The myth of "a frail and helpless woman," on the other hand, is promoted to ensure full reliance on the male sex.³

Women's and girls' violence is a significant health and human rights problem. At some point in their lives, at least one in every five women in the world has been physically or sexually assaulted by a man or men. Many people, including pregnant women and young girls, are victims of serious, long-term, or recurrent attacks. Violence against women is estimated to be as severe a cause of death and incapacity among women of reproductive age as cancer, and a greater cause of illness than road accidents and malaria combined around the world.⁴ Women's violence is effectively tolerated in almost every culture on the planet. When opposed to the number of attacks, men who beat or attack women or girls are rarely prosecuted and convicted. As a result, violence is used to preserve and perpetuate women's subordination. Description from the "*United Nations, The United Nations General Assembly adopted the Declaration on the Elimination of Violence Against Women in 1993*"⁵, which defines violence against women as "any act of gender-based violence that results in, or is likely to result in, physical, sexual, or psychological harm or suffering to women, including threats of such acts, coercion, or arbitrary deprivation of liberty, whether occurring in public or private, whether occurring in public or private." Physical, sexual and psychological violence occurring in the family, including battering, sexual abuse of female children in the household, dowry related violence, marital rape, female genital mutilation and other traditional practices harmful to women, no spousal violence and violence related to exploitation; physical, sexual and psychological violence occurring within the general community, including rape, sexual abuse, sexual harassment and intimidation at work, in educational institutions and elsewhere; trafficking in women and forced prostitution; and physical, sexual and psychological violence perpetrated or condoned by the state, wherever it occurs.⁶

The United Nations (UN) and its members were initially perplexed by transgressions against women and the fight against intolerances. They couldn't figure out if a breach of a

³ Indira Sharma, *Violence against Women: Where are the Solutions*, 57(2) Indian Journal Psychiatry 132 (2015).

⁴ Awadesh, *supra* note 2 at 2.

⁵ Declaration on the Elimination of Violence against Women, A/RES/48/104.

⁶ Guruappa Naidu, *Violence against women in India* 23 (Serials Publication, New Delhi, 2011).

woman's right could be considered a universal or a specific issue. Since the number of crimes against women is increasingly growing, women's rights are regarded as distinct rights that are well-managed by professional bodies.

The key goal of the United Nations and the “*United Nations Declaration of Human Rights, 1948*”⁷ was to create effective international licit instruments to promote egalitarianism and encourage just and fair justice for women. Fair rights and opportunities for men and women are at the heart of the Universal Bill of Human Rights. The privileges set out in this agreement apply to all, regardless of gender.⁸

In the Indian Constitution's Preamble, Fundamental Rights, Fundamental Duties, and Directive Principles, the principle of gender equality is enshrined. The Constitution not only guarantees women's equality, but also empowers the government to take constructive discrimination steps in their favor to offset the accumulated socioeconomic, educational, and political disadvantages they face. Our legislation, development policies, plans, and programs have all sought to advance women in various fields within the context of a democratic polity. India has also ratified a number of international conventions and human rights instruments that contribute to ensuring women's equality. The ratification of the “*Convention on the Elimination of All Forms of Discrimination against Women (CEDAW)*”⁹ is one of the most significant.¹⁰

1.1 Overview of violence and violation of human rights against women in India:

In India, women are subjected to a variety of forms of abuse. There are unfamiliar forms of violence, such as sati, dowry death, female infanticide, acid attack, and witch hunting, in addition to common types of violence such as domestic violence, sexual assault at work, and rape. There are also trends that, while not violent in and of them, rob women of their rights and a decent future and are likely to turn violent. Child marriage, purdah, and the ban on widow's remarriage are among them.¹¹

⁷ UN General Assembly, Universal Declaration of Human Rights, 10 December 1948, 217 A (III).

⁸ Niamh Reilly, *Women's human rights Seeking Gender Justice in a Globalizing Age* 44 (Polity Press, 2009)

⁹ UN General Assembly, *Convention on the Elimination of All Forms of Discrimination Against Women*, 18 December 1979, United Nations, Treaty Series, vol. 1249, p. 13.

¹⁰ India, Ministry of Statistics and programme Implementation, *Women and Men in India 2012*, 14th Issue, p. xiii

¹¹ Mala Sen, *Death by Fire: Sati, Dowry and Female Infanticide in Modern India* 10 (Phoenix, 2002).

Honour Killings: In some parts of the world, is a popular type of violence against women. Honour killings are murders committed by family members (usually husbands, fathers, uncles, or brothers) against women in the family who are thought to have brought the family dishonor. The dishonorable woman's death is thought to restore honor. These killings are a long-standing phenomenon that is thought to have evolved from tribal practices in which a single accusation against a woman may be enough to ruin a family's reputation. Women are killed for a variety of reasons, including refusing to accept an arranged marriage, being in a relationship that their family disapproves of, trying to leave a marriage, having sex outside of marriage, being a victim of abuse, and dressing in inappropriate ways. Honor killings are most often associated with the Middle East and South Asia, but they can occur anywhere in the world. Honour killings are prevalent in India's northern states, especially Punjab, Haryana, Bihar, Uttar Pradesh, Rajasthan, Jharkhand, Himachal Pradesh, and Madhya Pradesh. In Turkey's south-eastern Anatolia, honor killings are a severe issue.

Dowry Death: Dowry is a property that a bride gives to her husband's family when they marry. The Dowry Prohibition Act, enacted in 1961, makes it illegal to carry a dowry, but it has almost no effect. When a husband's family is dissatisfied with the amount of dowry, the wife will be raped, and it is not uncommon for a wife to commit suicide or be killed as a result of the intolerable violence. Murders involving dowry, such as brides being burned to death (so-called dowry killings), have been recorded. However, since such killings are often disguised as suicides by suspects, the authorities treat many incidents as suicides.

Obscenity & Pornography: Pornography is written or visual content that contains the explicit description or exhibition of sexual organs or behavior, and is intended to induce sexual arousal or appears lewd to a responsible reader. The representation of sexual subject matter for the purpose of sexual arousal is known as pornography. Pornography can be found in a number of forms, such as books, magazines, postcards, photos, sculpture, illustration, painting, animation, sound recording, film, video, and video games, as well as websites. The proliferation of illicit websites containing obscene and pornographic materials has resulted from the increased usage of information technology, such as the Internet and communication devices. The Indian Penal Code, 1860, and the Information Technology Aact, 2000 do not have clear definitions for obscenity and pornography.

Sati: Sati is a Hindu funeral custom in which a newly widowed woman immolates herself on her husband's funeral pyre, either willingly or through the use of force and coercion. It has been illegal since 1892, when Britain ruled the world. However, in 1987, an eighteen-year-old widow named Roop Kanwar was claimed to have been burned to death at her husband's funeral, prompting the re-enforcement of the Sati Prohibition Act. This method, however, has not been fully eliminated.

Female Infanticide: The sex ratio of infants aged 0 to 6 is 1,000 males to 927 females, according to the Indian Census of 2001. The ratio was 1,000 to 976 in 1961. Clearly, the female birthrate and/or child survival rate are on the decline. "Provisional data released by the census office of 2011 shows that child sex ratio has further declined to 914 girls every 1000 boys as compared to 927 in 2001."¹² Male infants are traditionally favoured over female infants, and female infants are heavy financial burdens for the family due to dowry. Many female babies are murdered by their parents before or after birth: aborting a female fetus as a result of prenatal diagnosis is a current practice.

Acid Attacks: When women refuse to obey men's commands, they are subjected to acid attacks as a form of punishment. It may happen to significant others as well as non-significant ones. Acid is often smeared on women's faces in order to degrade their beauty by obliterating their most feminine features. The attack causes serious damage, such as deforming faces and skin to the point that the original features can no longer be recognized.

Witch Hunting: It is a practice in which certain women are accused of being witches and are severely raped, tortured, killed, forced to commit suicide, or chased away from their villages. Witches are women who have no children, are widows, and engage in their own economic activities; in other words, they do not fulfill the traditional roles that women are supposed to fulfill. In tribal cultures, witch hunts are popular.

Child Marriage: Despite the fact that child marriage has been illegal since the British government passed a law prohibiting it in 1929, the practice is still widely practiced in India today. Recently, child marriage has been highlighted as harming women's welfare throughout their lives and creating a vicious cycle: young girls are denied an education, and this lack of

¹² Rukmini Shrinivasan & Himanshi Dhawan, *Sense of Census 2011: Save the Girl Child*, TOI, Apr. 1, 2011.

education leaves young wives who are victims of domestic violence (DV) without a sense of human rights. Underdeveloped women bear unhealthy babies, unhealthy mothers raise frail children, and these children marry young as well.

Purdah: Purdah, which literally translates to "curtain" in Persian, is a South Asian tradition of segregating women. Separating women from the rest physically, covering their bodies with fabric outside of their homes, and covering their bodies and saying no words except at home if wives are in front of many people and strangers from the husbands' family are all part of the ritual. It was popular among Hindu women from high castes in North and East India, not just among Muslims. Purdah, on the other hand, is practiced by some families from lower castes in order to increase their social status by imitating a high-class tradition. Purdah is still performed today in the guise of tradition and culture. It keeps women from getting out in public and becoming involved, as well as increasing their reliance on men and male dominance.

The ban on widows remarrying: The prohibition of widow's remarriage was a regulation among high castes such as Brahmin in 19th century Hindu society. Women in Hinduism are expected to serve only one man during their lives. Widows were also economically dependent on others to feed them, and they faced discrimination and disrespect in society. Also, similar to purdah, people from lower castes often forbade widows from remarrying in order to elevate their social status. Similarly, high-ranking Muslims discouraged women from remarrying, despite the fact that Islam does not have such a rule. Under British rule, the Hindu Widow's Re-marriage Act was enacted in 1856.

Forced Marriage: Is a marriage in which one or both of the parties is married against their will. In South Asia, the Middle East, and Africa, forced marriages are normal. Bride price and dowry rituals, which are common in many parts of the world, contribute to this practice. A forced marriage is often the result of a family feud that is resolved' by the transfer of a female from one family to the other.

Widow's Mistreatment: Drafters should understand that widows' mistreatment covers a wide range of human rights abuses. Domestic abuse, sexual harassment, forced marriage, prostitution, property grabbing, property transfer, forced evictions, and discrimination against women in regard to marriage, its breakdown and divorce, property and land rights, children, and

inheritance are all issues that widows face. All of these types must be addressed and prohibited by civil and criminal legislation, which must also protect women's and girls' rights, provide a legal recourse, and ensure accountability for offenders.

Forced Evictions and Exclusion: Following the death of their husbands, widows in India are often evicted from their matrimonial homes and left alone to feed themselves and their children. In almost all countries, whether developed or developing, legal protection of tenure for women is almost entirely dependent on the men with whom they are associated, according to the UN Special Rapporteur on Adequate Housing. Women in general, and women who run households, are much less safe than men. Women own very little property. A woman who is separated or divorced and has a family to support sometimes ends up in an urban slum, where her security of tenure is at best suspect. There is mounting evidence that in poor families, women spend more on basic family needs, while men spend a large portion of their income on personal products such as alcohol, cigarettes, and other vices.

Sexual Harassment at Work: The Supreme Court's Vishaka guidelines in 1997 kicked off a national conversation about sexual harassment of women at work in India. The passage of the Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013¹³, on the other hand, aided in the translation of these guidelines into specific rules to be followed. The problem of sexual harassment has largely been swept under the carpet in India, says the study. Because of social taboos still associated with sexual abuse, the laws have never been effectively invoked. In India, women face discrimination when it comes to receiving remuneration for their work. This is true in both urban and rural settings. Women entrepreneurs face more challenges when it comes to obtaining credit to start their own companies.

Female Genital Mutilation: Female Genital Mutilation (FGM) is a term that refers to non-medical operations that include partial or complete removal of the external female genitalia or other injuries to the female genital organs. Adult and married women are rarely subjected to this treatment, which is often performed on girls between the ages of one and fifteen. This is a traditional practice among the Bohra community in India, where the ritual is known as "Khatna" or "Khafz/Khafd." Khatna is the practice of cutting the tip of a girl's clitoris when she is between

¹³ Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013, No. 14, Acts of Parliament, 2013 (India).

the ages of 6-7 years old¹⁴. Mullanis-women with a semi-religious background, conventional cutters, or any woman with some experience perform it. According to an online survey conducted by Sahiyo, an NGO among Bohra women, 80 percent of the 400 respondents have gone through the khatna process.¹⁵

FGM is carried out for a variety of socio-cultural factors that differ from region to region. Both of these factors, however, are rooted in deep sexism against women and children. Religious dicta, an aid to female hygiene, and a means to regulate or reduce female sexuality are among the different justifications for FGM that have been advanced. The practice is often related to a rite marking the coming of age and initiation into womanhood in many countries.¹⁶ The key reasons for the flourishing practice, according to a study conducted among women of the Dawoodi Bohra community, were religious requirements, traditions and customs, and the desire to curb the girl's sexuality.

FGM is often viewed as a method of purging a girl of impure thoughts and desires. A circumcised girl is thought to be less aroused than one who is in 'qalfa' (meaning with a clitoral hood) or whose clitoris is intact. Girls and women's sexual appetite is seen as something they need to be protected from. This perceived security extends beyond the girl's personal safety to the integrity of the entire family. The belief that the clitoral head is "unwanted flesh" or a "source of sin" that will cause them to stray from their marriages is at the heart of a tradition that predates Islam but thrives among Bohras in many places. Some women referred to the clitoral hood as an "immoral lump of flesh," or "haraam ki boti."¹⁷

FGM has both short and long-term negative consequences for the victim's health and psychological well-being. The severity of the cutting/mutilation is proportional to the damage sustained. There is a lot of discomfort because anesthesia is rarely used on the victim during the operation.¹⁸ Excessive bleeding, swelling, and inflammation in the genital region, infection,

¹⁴ Harinder Baweja, *India's Dark Secret*, Hindustan Times, <https://www.hindustantimes.com/static/fgm-indias-dark-secret/>.

¹⁵ *Id.*

¹⁶ UNFPA, *Implementation of the International and Regional Human Rights Framework for the Elimination of Female Genital Mutilation*, UNFPA (Nov, 2014), <https://www.unfpa.org/sites/default/files/pub-pdf/FGMC-humanrights.pdf>.

¹⁷ Harinder, *supra* note 13.

¹⁸ WHO, *Female Genital Mutilation*, WHO, https://www.who.int/health-topics/female-genital-mutilation#tab=tab_1.

urinary problems, and, in some serious cases, deaths are among the other short-term health risks. Chronic genital infections, recurrent urinary tract infections, painful sexual intercourse, complications during pregnancy, labor and delivery of the infant, prenatal risks, and crippling psychological effects such as post-traumatic stress disorder (PTSD) and depression are among the long-term consequences. FGM has a negative impact on girls' and women's health and social growth. In contrast to male circumcision, FGM has no health benefits.

CHAPTER 2

CAUSES AND CONSEQUENCES OF VIOLENCE AGAINST WOMEN

2.1 Reasons for Crime against Women and their Consequences:

Women are seen as the weaker members of society. As a result, they are subjected to various forms of abuse. During conflict between two groups or cultures, they become the easiest target and victim. Owing to their weaker positions, they are powerless to fight oppression. It has become their habit to suffer in silence both inside and outside their homes. Rape and sexual assault are used to teach hostile groups a lesson. Women are the first and easiest targets during communal or caste riots. Teasing or bullying women may often act as a catalyst for two aggressive groups to clash, resulting in abuse.

The low status of women in our society is one of the causes of rising crime against women. Women's views have remained largely unchanged. They are viewed as a burden, and as a result, they are refused an education. According to the 1991 Census, women have a literacy rate of 39 percent compared to 63 percent for men. On the front of literacy, the situation among women from lower castes is troubling. In some nations, it's even smaller than 39 percent. The sex ratio has decreased from 933 in 1981 to 929 in 1991, indicating a decrease in the number of girls born, which is a sad state of affairs. Women are treated as if they were commodities. They are dealt with as if they were assets. They are unquestionably taken for granted. Efforts have been made to make women dependent on the men. They are also economically dependent, which has exacerbated their predicament.¹⁹

It is now commonly recognized that girls are emotionally closer to their parents, are more responsible in society, and are not in any way less capable than boys. Despite this, the traditional Indian mindset, which is influenced by a variety of socioeconomic and cultural factors, has often supported the birth of a male child and discouraged the birth of a female child in the family. This has greatly contributed to the rapid growth of female feticide in India, making it one of the

¹⁹ John Marshall Macdonald, *Rape Offenders and Their Victims* 276 (Charles C. Thomas Publication Ltd., 1st ed., 1971).

world's most skewed sex ratio-affected countries.²⁰ The following are the most important factors that encourage crime against women in India:

Factors of Religion: The Hindu religion places a high value on the birth of a son. In a Hindu patriarchal society, the family lineage, or 'Vansh,' is carried on by the son. A man cannot achieve moksha, according to Manu, unless he has a son to light his funeral pyre. It also states that a woman who gives birth to only daughters in her eleventh year of marriage may be abandoned. Gender-biased rituals and traditions in traditional Hindu culture have over-emphasized the birth of sons thus discouraging the birth of a girl child, paving the way for Female Feticide.²¹

Dowry's Evil: Dowry is fundamentally one of the reasons that has greatly aided the practice of Female Feticide. Parents believe that avoiding female fetuses is a safer choice than paying exorbitant prices in the form of 'dowry' when marrying off their children. As a result, in order to avoid dowry, people resort to sex selection tests in order to exclude the female fetus. Most couples, particularly those from the middle class, tend to believe that "paying Rs. 500 now is better than paying Rs. 5,00,000 later." In contrast, the boy is seen as a valuable asset capable of bringing in a large dowry for the parents. As a result, boys naturally outnumber girls.

Financial Dependence of Females: In India, the tragic female feticide has also been blamed on socioeconomic factors. Certain communities seek to eliminate female children who are forced to live in dehumanizing conditions such as poverty, education, superstition, and illiteracy. Some men are unable to see women succeeding because they are unemployed or underemployed. They blame those women for their shortcomings, and they harbor a grudge against them, committing crimes against them to vent their rage. There have been instances where husbands have not even left their wives to vent their frustrations, despite the fact that she is the breadwinner for the entire family. They imagine the wife mocking or looking down on them when they are at home without a job because they are dependent on her. They imagine her having fun at work with other guys. Unemployed men have been caught slapping their wives over minor domestic disputes.

²⁰ R Geetha Gowri, *Elderly Women: A Study of Unorganized Sector 92* (Discovery Publishing Pvt. Ltd., 2003).

²¹ Saumya Kaushik, *Women Welfare: Some New Dimensions 491* (Sarup & Sons, New Delhi, 2003).

Women's Status: Sons are typically expected to carry on the family legacy, provide protection and care to parents, especially in their later years, increase family wealth and property, and perform last rites and rituals. Daughters, on the other hand, will go to another's house and drain the family's money. Furthermore, they must always be protected, defended, and cared for, putting an additional burden on the family. One of the most powerful factors that has caused strong son preference and thus promoted Female Feticide is the conservative mindset of Indian society, which basically treats women as a "burden." All of these factors point to the fact that our country's long-standing gender inequality in favour of men, as well as the stereotype of women as a "burden," is the driving force behind India's alarming figures on female feticide.

The Personal Causes: Female offenders have a lower level of education than male offenders. Many female criminals are illiterate or only partially literate. They lack social awareness and experience, as well as poor survival skills. They lack practical problem-solving capabilities and are unable to make rational decisions. When they are provoked or enticed by others, it is simple for them to be coerced or misled, leading them astray and into a life of crime. Because of their lack of experience, they have a limited understanding of the law. They cannot look at and fix problems from a legal perspective when they have been violated by unlawful infringements, so they resort to severe, aggressive, and lawless solutions. Some women, for example, are victims of domestic violence but have no idea how to use the law to defend them. They fight violence with violence, and if they can't stand it any longer, they'll destroy the perpetrators. There will be offenders as well. Furthermore, psychological factors such as arrogance, unrealistically comparing, hedonism, narrow-mindedness, vindictiveness, and so on play a role in female crime.

Gender Based Abuse: There are many types of violence against women, including state-sanctioned, community-sanctioned, and family-sanctioned physical, sexual, and psychological violence.²² Gender-based violence includes: gender-based killings; rape and sexual violence; forced marriage – including child marriage; sexual harassment in workplaces, schools, and public places; female genital mutilation and other harmful practices; trafficking and online violence against women; economic violence, including dowry abuse; and psychologic violence. Perpetrators are more likely to target women and girls who are further disadvantaged because of

²² R Geetha, *supra* note 19 at. 687.

other facets of their sexuality, such as living with a disability or being gay, bisexual, or transgender women and girls.²³

These types of violence are diverse, but they are also linked. For instance, child marriage, which occurs in all parts of the world, is linked to higher levels of domestic abuse, including rape within marriage and by recognizing that perpetrators target girls and women of various ages for various types of abuse, the life-cycle approach sheds more light on the various forms of gender-based violence.

Lack of Public Safety: Outside of their homes, women are usually unprotected. The gang rape happened on a bus, and even Indian authorities admit that public spaces in the country can be dangerous for women. According to a new study from the Ministry of Women and Child Development, several streets are poorly lit, and there aren't enough women's restrooms. Women who drink, smoke, or frequent pubs are generally regarded as morally sloppy in Indian culture, and village clan councils have blamed an increase in the incidence of rape on a rise in women talking on mobile phones and going to the bazaar.

Rape Victims Are Encouraged To Compromise: A 17-year-old Indian girl who was reportedly gang-raped killed herself after police forced her to drop the case and marry one of her attackers in a separate rape case. Village leaders and clan councils also urge rape victims to "compromise" with the accused's family and drop charges, or even marry the rapist. Compromises like these are made to maintain peace between families or clan groups. Furthermore, it is thought that a girl's chances of marrying are more significant than taking a rapist to justice.

Alcoholism: It has been one of the leading causes of female-on-female abuse. This evil is quickly spreading across society. Alcohol's negative effects include significant harm to the mind and body, as well as an increased risk of crime. Excessive drinking leads to family member malnutrition, as well as assaults and quarrels between husband and wife, father and boy, desertion, beating, cruelty, and other issues. In a state of emotional enthusiasm, habitual drunkards have even molested their own daughters; when a person's usual constraints vanish under the influence of narcotics or alcohols, and their hostile and aggressive fantasies, closely

²³ Saumya, *supra* note 20 at. 199.

entwined with sexual desire, are transformed into reckless action. Alcohol-related offenses show a blatant disregard for time, space, and situation.

Marital Maladjustment: This aspect is the result of a significant number of crimes committed against women. The transition of the girl who joins their in-laws' family, their jobs, and the enlightened one is extremely difficult. Mothers-in-law who have complete power over their family members are jealous and irritated by their daughter independence. Indian husbands place a higher value on their mothers informing them of their wives' protests. Temperamental maladjustment and incompatibility in forms of thinking, living, dressing up, and acting play a significant role in the development of schizophrenia. As a result, the husband neglects his wife or becomes preoccupied with quarrels or minor problems. He would often abandon his wife or turn to prostitution to fulfill his desires.

Gender Schemas and Attitudes: At the person level, attitudes and gender schemas reflect cultural stereotypes about crime, gender scripts and roles, sexual scripts and roles, and male entitlements. These hypothetical entities are expectancies that provide a context for the spectrum of potential responses, as well as giving meaning to and possibly biasing understanding of ongoing experience. A wide range of Americans, including ordinary people, police officers, and judges, have shown acceptance of views that have been shown to promote rape. Men are more likely to misinterpret contradictory data as supporting their views once they have established a violence-supportive schema about women.²⁴ Formally violent men are more likely than nonaggressive men to support a range of pro-rape views, such as rape myths and the use of interpersonal violence as a conflict-resolution strategy. Rape myths and beliefs can serve as justifications for those who commit violent acts. For example, imprisoned rapists often justify their actions by claiming that their victim either wanted or deserved to be subjected to unwanted sexual acts. Similarly, traditionally, culturally sanctioned assumptions about a husband's rights and privileges have legitimized a man's dominance over his wife and justified his use of violence to dominate her.²⁵ Men are more accepting of men exploiting women in general, with the most religiously conservative men being the most accepting.

²⁴ Rama Mehta, *Western Educated Hindu Women* 93 (Asia Publishing House, 1970).

²⁵ K. Gill, *Hindu Women's Right to Property in India* 95 (Deep & Deep Publications, New Delhi, 1986).

Morbidity in Psychiatry: There is strong evidence to indicate that alcohol has been linked to the commission of many types of VAW. A recent meta-analysis found clear evidence of a connection between alcohol and female intimate partner abuse. Aggression is more common in psychiatric patients, particularly those with serious mental illnesses like schizophrenia. More rage is experienced by people with the most pathological cluster type personality. Some psychiatric disorders, such as psychotic schizophrenia, delusional disorder, bipolar disorder, and antisocial personality disorder, have been related to sexual VAW.²⁶

Sexual harassment is more common in people with intellectual disabilities than in the general population, making them an especially vulnerable group. Women suffering from depression, chronic mental illness, or mental retardation, for example, may be particularly vulnerable to different forms of violence.²⁷

Women suffering from serious mental illness are a particularly vulnerable group who are at risk of different forms of abuse. Because of the pervasive stigma associated with mental illness, women with mental illness are often rejected by their families, particularly when the illness manifests soon after marriage or the fact of mental illness before marriage is discovered. A serious, chronic, and debilitating mental disorder is a basis for nullity of marriage, according to Indian legislation such as the Hindu Marriage Act, 1955²⁸, and the Special Marriage Act, 1954²⁹. As a result, many husbands abandon their mentally ill spouses because they know they can always remarry in a patriarchal society. However, since many of these women are married with a large dowry and because marriage is viewed as a permanent union, the women and their families may take a variety of steps to prevent the marriage from being null.

As a result, if social measures fail, legal action can be taken. Complaints can be filed under the Dowry Prohibition Act³⁰, the PWDVA, or Section 498A of the Indian Penal Code (of cruelty by husband and relatives of husband). While complaints of dowry abuse and/or harassment are made in these situations, the main issue is the restoration of conjugal rights, not dowry. In most cases, dowry isn't a problem since both the giver and the recipient of dowry were

²⁶ Neena Bohra, et al., *Violence against Women*, 57(2) Indian J. Psychiatry 1-2 (2015).

²⁷ *Id.*

²⁸ The Hindu Marriage Act, 1955, No. 25, Acts of Parliament, 1955 (India).

²⁹ The Special Marriage Act, 1954, No. 43, Acts of Parliament, 1954 (India).

³⁰ The Dowry Prohibition Act, 1961, No. 28, Acts of Parliament, 1961 (India).

in agreement. Women may be subjected to various types of abuse in order to force them out of their marriages. It's almost always a lose situation. The treatment of women's mental illnesses has been ignored throughout, worsening the crisis and closing the door to reconciliation. Many marriages end in divorce or breakup, with children bearing the brunt of the pain.³¹

Motives of Sex and Power: Women's violence is thought to be driven by a desire to control them. This perspective conjures up images of a strong man using violence against women to preserve his dominance, but research shows that the relationship is more nuanced.³² Intimate partner violence is often motivated by power and influence, but it may also be motivated by a man's feelings of powerlessness and unwillingness to acknowledge rejection. It has also been suggested that rape, in particular, satisfies sexual desires through abuse, but research has shown that power and rage motivations are more common in rationalizations for sexual assault than sexual desire. Laboratory studies of men's sexual arousal to stimuli depicting pure aggression, pure consensual sex, and non-consensual sex plus violence have been used and try to settle the sex versus power controversy.

These studies have consistently shown that rape stimuli involBottom of Formving adult women can arouse some “normal” males with no known history of rape, particularly if the women are depicted as enjoying the experience. Sexually violent men, on the other hand, tend to be more sexually arousal in general, whether to consenting or rape, and rapists respond to rape cues more than nonsexual offenders to consenting sex cues. Sexually violent men freely admit that aggressive and sadistic content dominates their sexual desires.

Learning in a Social Context: Humans learn social behavior by watching others' actions and the effects of those actions, developing ideas about what behaviors are acceptable, trying those behaviors, and continuing those if the results are good, according to social learning theory. Aggression is not viewed as inevitable in this theory; rather, it is viewed as a social activity that is learned and conditioned by its effects, and that continues if it is reinforced.

Male violence against women persists in human cultures, according to this view, since it is modeled both in individual families and in society at large, and it produces positive outcomes:

³¹ Neena, *supra* note 25.

³² R Geetha, *supra* note 19 at. 35.

it relieves stress, makes the perpetrator feel better, frequently achieves its goals by cutting off appeals, and is seldom associated with severe punishment for the perpetrator.

Early Marriage: Married teenage girls with low levels of education are more likely to experience social alienation and domestic violence than women who marry later in life. Girls often move to their husband's home after marriage to take on the domestic function of being a wife, which often necessitates relocating to a different village or town. A young girl may drop out of school, move away from her family and friends, and lose the social support she once had as a result of this transition. Because of her youth, a husband's family will have higher standards for the girl's submissiveness to her husband and his family. This feeling of being cut off from others may have serious mental health consequences, including depression.

Domestic abuse and marital rape are more likely when there is a large age difference between the child and her spouse. Girls who marry as children are more likely to experience serious and life-threatening marital abuse. In child marriages, husbands are often more than ten years older than their wives. This can give a husband more power and influence over his wife, contributing to the prevalence of spousal abuse. Early marriage puts young women in a vulnerable position where they are totally reliant on their husbands. Since young girls are in a formative stage of psychological growth, domestic and sexual abuse from their husbands has permanent, damaging mental health implications for them. Depression and suicidal thoughts are two of the mental health effects of spousal abuse. In the homes of their husbands and in-laws, child brides face social isolation, emotional violence, and prejudice, particularly in situations like vain.

Domestic Violence Acceptance: India was rated one of the worst countries in the world for women by the Reuters Trust Law community this year, in part because domestic abuse is sometimes seen as justified. According to a UNICEF study from 2012, 57 percent of Indian boys and 53 percent of Indian girls aged 15 to 19 believe wife-beating is justified. According to a new national family-health study, a large percentage of women blame themselves for their husbands' beatings.

Painful Crime Reporting: Improving the reporting of violent crimes against women in India is a significant move forward.³³ For a few courageous souls try to take that initiative while battling different forms of social sanctions, the next challenge they face is grappling with the authorities' insensitivity.

Society of Patriarch: It has been identified as the primary source of female-on-female crime. Women who have a higher economic status than their husbands and are perceived to have enough power to alter conventional gender norms are at a higher risk of abuse.

³³ Lina Gonsalves, *Women and Human Rights* 213 (APH Publishing Corporation, 2008).

CHAPTER 3

VIOLENCE AGAINST WOMEN IN KASHMIR

3.1 Introduction:

Women in Kashmir have gained financial freedom and a sense of empowerment as a result of increased education and job opportunities, but they have also become trapped in a vicious cycle of domestic violence. Domestic violence has increased dramatically in the Kashmir Valley over the last decade, according to sociologists, activists, and legal experts, and is directly related to outrage over women's newly gained autonomy in the area, which has broken men's traditional stranglehold on the household and economy. An analysis of violence against women is a topical study that depicts the condition of the majority of women who work at home. Violence against women is described as "any act of gender-based violence that results in, or is likely to result in, physical, sexual, or psychological harm or suffering to women, including threats of such actions, intimidation, or arbitrary deprivation of liberty, whether occurring in public or private life," according to a United Nations study. Kashmir is a thorn in India's side. Kashmir is our first priority when we make a plan to explore the country. The beauty of the mountains and the taste of nature still draw you to Kashmir. Women and nature are inextricably linked. Women are often valuable to the earth; their existence imbues nature with a sense of strength and integrity. Women respect their serotype status in society and strive to prove themselves in war or at the kitchen table. Kashmir is a place created by God's grace, but its people, especially its women, are still denied their basic rights. Bilal Bashir Magry claims that with each passing day, he becomes more persuaded that Hurriyatization is the greatest prize of Kashmir's freedom struggle. Women played a critical role in our culture, but they were largely ignored. If anyone wants to overthrow a society, all they have to do is concentrate on their female power and they'll get what they want. Domestic violence is on the rise in the Kashmir Valley, according to a survey, with studies revealing that more than 40% of Kashmiri women are physically or mentally abused by their husbands or in-laws.³⁴

³⁴ Rahul Kumar, *A Study of violence outside and inside against woman in Kashmir*, 3 UGC National Conference 2 (2016).

In Kashmir, the fact of Indian democracy is revealed in a way that no nationalist Indian wants to hear. The Indian state stripped Kashmir of Article-370 on August 5, 2019,³⁵ followed by daily crackdowns on the internet (4G network is yet to be restored) and phone networks, travel restrictions, prolonged lockdowns, and other measures to make Kashmiri life even more difficult. Furthermore, the embarrassment that people face at army and police checkpoints, as well as surveillance, intimidation, blockades, unlawful detentions, and profiling, has become a gruesome but commonplace fact of their daily lives.

3.2 Many Faces of Violence in Kashmir:

Patriarchy has long been an instrument of oppression and injustice toward women, culminating in numerous types of gender-based abuse, dating back to ancient times. It occurs in all environments, including the workplace, the home, the streets, and the society at large, as well as in armed conflict circumstances, and is committed by men. The most important truth is that women and girls are overwhelmingly victims of abuse perpetrated by men they know and inside the so-called "protected heaven" of their homes and families. Gender power disparities and other inequalities play a significant role in the dynamics of violence in all of these cases. Women in Kashmir share the same sorrows and fortunes as women in other parts of the world, despite the fact that infanticide, foeticide, and dowry deaths are not practiced. Women in Kashmir are commonly exploited and maltreated, subjugated, and physically victimized right from childhood due to socially organized injustice.³⁶

Women in Kashmir share the same joys and sorrows as women in other parts of the world. Despite the fact that infanticide, foeticide, and dowry deaths are not common, women are often raped, maltreated, subjugated, and physically victimized from a young age as a result of socially structured injustice. Furthermore, because of the evolving social system, they are now vulnerable to all forms of sexual assault. They are subjected to crimes such as sexual assault, molestation, eve-teasing, and even unethical trafficking, kidnapping & abduction, and rape, as shown by police reports, which, due to underreporting, only constitute a small portion of the

³⁵ IANS, *Striking down Article 370 tipping point, say Kashmiri Pandits*, India Today, Aug. 14, 2019.

³⁶ Aneesa Shaifi & Mohmad Saleem Jahangir, *Women at Risk: Understanding Power and Violence in Kashmir*, 2(1&2) Social Work Chronicle 1 (2013).

actual victimization of women. Furthermore, during the conflict in Kashmir, there has been a significant rise in sexual abuse against women.³⁷

The violence in Kashmir has gotten worse over the last three decades, with insurgency and militarization affecting daily life. Aside from the obvious physical violations, such as various rape cases against the Indian Armed Forces, as well as the killings of rebels and civilians, there are many overt consequences of the war, including the emotional suffering of living in a conflict zone.³⁸

Women's responses are diverse, reflecting the complexity of the dispute and its related daily struggles. Some women express themselves by taking an active role in political spaces, advocating for civil and political rights. While others are unwillingly compelled to take on new unusual positions (such as half-widows who are suddenly thrust into the public domain of conflict to take on non-traditional roles), for others, even stepping out alone to their orchards is too much of a risk to take as the accountability crisis in Kashmir's rural areas is even worse.³⁹

Leading a dignified life for half-widows in Kashmir (husbands abducted/disappeared by security forces or militants) can be a real challenge. Women's identities are entangled with their husbands' in a traditional Kashmiri culture, and once a woman is married off, she becomes the man's liability. As a result, many of these women (half-widows) and their children face a survival crisis due to a lack of resources. *“The lack of closure in their lives makes their life unbearable,” writes Nyla Ali Khan, an academic and Sheikh Abdullah's granddaughter. Nonetheless, it is these women's vulnerability that brings them together and encourages the formation of unity where they are connected through sorrow, struggle, and resistance.”*

Although the sight of women looking for their sons, brothers, or husbands outside army camps/police stations is heartbreaking, it also exposes women to the worst kind of public sphere in a conservative and militarized society. The women are not only suspected of being state informants in these situations, but they are also harassed by the male-dominated bureaucratic system. Furthermore, the large presence of Indian troops, who are seen as an occupying force by

³⁷ Aneesa, *supra* note 35 at 2.

³⁸ *Id.*

³⁹ Zohra Batul, *Indian Apathy and Systemic Violence against women in Kashmir*, LSE – Engenderings, <https://blogs.lse.ac.uk/gender/2020/09/14/indian-apathy-and-systemic-violence-against-women-in-kashmir/>.

the locals, causes fear among women and their families, resulting in women's movement being limited in public spaces. It has, in turn, culminated in an overabundance of power over women and their bodies.⁴⁰

In 2011, 15,000 Indian women were purchased and sold as brides in areas where foeticide had resulted in a scarcity of females. The population of Kashmir, a northern Indian state, has decreased from 900 in 2001 to 883 in 2011. Daughters have also been seen as a burden and a liability in society in northern India. Brides being murdered for lack of dowry are a regular occurrence. As a result, having a girl child is a bad omen for the family. A deep rooted traditional son preference, continued practice of dowry, concern for the protection of the girl child, and exploitation and abuse of women and girl children are among the reasons for the high number of cases of female foeticide in India, especially in Jammu and Kashmir. Any of the truth around female foeticide can be attributed to the women's being treated unfairly.

Inadequate education is also a major contributor. Female foeticide is one of the most serious problems of the twenty-first century, and it must be discussed and dealt with effectively by humanity. Female Foeticide, if allowed to continue at its current pace, would undoubtedly result in a slew of social issues in the immediate future. Due to a scarcity of female sex, the number of cases of rape, molestations, and the spread of homosexuality in society would skyrocket. Men and women cannot be in conflict with one another for the growth and advancement of mankind and the prosperity of humanity; rather, they must work together in coordination and collaboration, since they are incomplete without one another. As a result, saving the girl child becomes critical, as man cannot succeed on his own in the long run. It is our responsibility as civilized people to speak out against the worsening sex ratio and the killing of girl children. As women, it is our primary responsibility and concern to come forward and put an end to this threat.

3.3 The Apathy of Indian Audience:

With the exception of a few Indian academics, the Indian people bear no political or moral obligation for the women of Kashmir. This does not mean that they are uninterested in the Kashmir issue; in reality, for many Indians, Kashmir has become a source of national pride as

⁴⁰ Zohra, *supra* note 38.

well as personal concern, with many claiming that Kashmir is India's atoot ang (internal part). However, when it comes to the grave crimes perpetrated against Kashmiris and the consequences for women's lives, they tend to remain in the dark. “The Indian public is not so sensitive towards anti-national Kashmir Muslims,” writes Balraj Puri, a journalist and human rights activist.⁴¹

In urban India, there is a distinct shift in attitude toward women's rights, as well as some trends toward feminist inclinations. This is not to say that there isn't widespread discrimination against women in India, especially among Dalits. However, there have been some social campaigns in India recently, such as the Me-too movement protesting rape and rape culture, the Sabarimala movement for spatial equality, and so on. When it comes to the appalling violence perpetrated against women in Jammu and Kashmir, however, the same society expresses great discomfort and duplicity. To take a recent example, some liberal groups staged a protest in Delhi, Aligarh, Mysore, and other cities in support of the Kathua rape and murder victim, only to downplay the context of the crime by framing it as yet another case of violence against women in India. The entire political machination behind the violent crime perpetrated by upper-caste Hindu men with the help of Hindu far-right groups to terrorize the Muslim Bakarwals (nomadic) community and push them out of Rasana (in Kathua) is largely ignored in mainstream Indian discourse. Even the ostensibly liberal segment of Indian society fails to understand that the rape cases of Kunan Pashpora, Shopian, and others cannot be comprehended without challenging the state's immunity given to the perpetrators.⁴²

On the other hand, in India's heartland, an objectified portrayal of a fair-skinned Kashmiri woman has become a familiar and casual part of everyday language. Bigotry against Kashmiri women is a common occurrence. I first heard it when our north Indian friends jokingly referred to Kashmiri men as Al-Qaeda, katwa (circumcised) for Muslim men in general, and Kashmiri musali (the word musali has several different meanings, but in this sense, it refers to Kashmiri Muslim women in a derogatory tone) for Kashmiri Muslim girls like myself. The sexist mentality that pervades Indian society was recently demonstrated in Tik-Tok videos of men swaggering about the prospect of marrying a Kashmiri woman following the repeal of Article 370 on August 5, 2019. Kashmiri women have long been exoticized, and the repeal of Article

⁴¹ Zohra, *supra* note 38.

⁴² *Id.*

370 has only exposed the Indian patriarchal fantasy of possessing the Kashmiri body further. The irony of the situation is that equal protection for women in Kashmir (a contentious topic in itself) was cited as one of the main reasons for the repeal of Article 370.⁴³

This 'sensationalization' of the Kashmir dispute has been sustained by the Indian public's complicity and the connection of Kashmir with Indian national pride. Even though Kashmir does not have a direct impact on India's elections, it does have an indirect impact. Following the Pulwama terror attack, the entire discourse surrounding the Indian election shifted to security, and then to Kashmir and terrorism. To make matters worse, the Indian media exacerbated bigotry by claiming that all is natural in Kashmir while simultaneously calling for vengeance against both Pakistan and the criminalized Kashmiris. Kashmiris have been harassed, fired from jobs, and evicted from their homes in Kolkata, Maharashtra (Yavatmal), and other cities.⁴⁴

The deep-seated discrimination against Kashmiri women and men in India can also be seen in the selective criminalization of Kashmiris. Ali Muhammad Bhat, Lattef Ahmad Waza, Mirza Nasir Hussain, who was wrongfully imprisoned for 23 years, and a Kashmiri couple in Delhi, Jahanzaib Sami and Hina Bashir, who were recently arrested on suspected ISI ties as it is simple to associate Muslim and Kashmiri labels with 'beard and burqa' as terrorists.⁴⁵

When a crime against humanity is committed in a regular and systematic manner, according to Hannah Arendt, it becomes banal. People support and justify the use of coercive measures to get back those who have supposedly lost their way or are mistaken, even at the expense of a massive humanitarian crisis, due to the banality of evil.⁴⁶

Indian leaders blame Pakistan for all of Kashmir's problems for a variety of reasons, including infiltrating and training militant groups, but attributing all of Kashmir's problems to Pakistan is misleading. Armed movement, street protests, stone pelting, poetry, literature, academia, and other forms of dissent against the Indian state are all actual, explicit, and everywhere. As a result, the state's need to justify its conduct in Kashmir is reduced by framing the Azadi movement as a manifestation of radical Islam and Kashmiris as troublesome.

⁴³ Zohra, *supra* note 38.

⁴⁴ *Id.*

⁴⁵ *Id.*

⁴⁶ *Id.*

Similarly, the narrow-minded Indian public discourse on violence against Kashmiri women, which views it exclusively through the lens of law and order or from the perspective of a women's rights narrative, does not help Kashmiri women. It only separates the structural violence perpetrated against them from the entire power principle of occupation, which is crucial in unraveling the political complexities of gender, faith, and conflict in Kashmir.

3.4 Sharp Rise in Domestic Violence & other Cases:

Domestic violence has been on the rise in the Valley at an unprecedented pace. Despite the fact that the majority of people in Kashmir deny the existence of domestic violence, recent reports and studies show otherwise. Owing to a variety of problems, the data available does not accurately depict the actual situation. The majority of women do not talk about it because they believe (or are led to believe) that it is their fate or kismet, and they must accept it. Many women may not consider such acts of violence to be violent if they feel they are justified. As a result, if the woman causes jealousy or fails to perform her wifely duties adequately, such as getting meals ready on time or adequately caring for children, wife beating is not seen as a severe response. This is complicated even further by the widespread perception that violent acts are simply an expression of love and a desire to help the subject become a better individual (International Center For Research On Women, 1999). Because of the embarrassment that would befall them and their families, many women are hesitant to file a lawsuit or a complaint of this type. Many people are afraid of the legal problems and headaches that come with the territory. Every year, the Women's Police Station in Ram Bagh records that over 2800 cases are filed. However, more than half of the participants have withdrawn due to family pressure or a settlement between the parties. According to sources, 550 cases were registered in 2013, with 3000 cases reported in 2014. On a daily basis, the police station receives over a dozen domestic violence reports.⁴⁷

The state government was forced to pass the Protection of Women from Domestic Violence Act (PWDVA) in 2010 as a result of an increase in domestic violence incidents.⁴⁸

Despite the fact that domestic violence against women is on the rise in Jammu and Kashmir, few attempts have been made to ensure that the Act is properly implemented. The state

⁴⁷ Sana Shafi et al., *The Scenario of Domestic Abuse against women in Kashmir*, 20 (9) IOSR 47 (2015).

⁴⁸ *Id.*

government appears to be too sluggish in providing effective security to aggrieved persons under the PWDVA, implying that the state is hesitant to keep its pledge as required by law. In 2012, Jammu and Kashmir's then-Minister of Social Welfare pointed to a shortage of funds as the reason for the Act's poor implementation. Furthermore, the State budget for 2014-2015 does not provide sufficient funds for the Act's proper implementation.⁴⁹

According to research, more than 40% of Kashmiri women are physically or emotionally abused by their husbands and/or in-laws. According to researchers, dowry, misunderstandings between the couple, and the birth of a girl child are all common causes of marital discord, which leads to a rise in domestic violence in the Valley. Unemployment and political instability in the Valley, among other things, are linked to the escalating violence, according to research. Every year, the State Women Commission of J&K receives about 1700 domestic violence complaints, the majority of which originate in the Kashmir Valley. According to the Commission's estimates, the Jammu area of the state has less domestic violence cases than the Kashmir valley. Domestic abuse, according to Dr. Mushtaq Margoob, a prominent psychiatrist in the Valley, is to blame for the majority of psychological problems among women in Kashmir. Suicide attempts are often prompted by women's vulnerability and loss of trust as a result of violence. Dr. Margoob also suggests that women who are victims of domestic abuse experience psychological anxiety, which has a negative effect on their mental wellbeing.⁵⁰

During the month of May this year, at least three women died as a result of domestic violence. Maroofa Begum, a resident of the Pulwama district, was admitted to the SMHS hospital after her in-laws allegedly set her ablaze. Maroofa died on May 15th, after a few days of battling for her life. Another woman from Shopian in south Kashmir died in the same hospital after setting herself on fire to avoid her husband's violence. In Uri, north Kashmir, a mother of four children was allegedly beaten to death by her husband and in-laws. Prof. B. A. Dabla, a well-known Kashmiri sociologist, attributes violence against women to patriarchal culture. Gender disparity, according to Prof. Dabla, is still prevalent in our culture. Here, there is still a

⁴⁹ Sana, *supra* note 47.

⁵⁰ *Id.*

lot of animosity toward women. Increased violence against women has arisen from the limited social and mental framework.⁵¹

The fact that domestic violence and harassment by in-laws is considered mostly a social problem is a major issue. The authorities only take care of the offense in exceptional situations, such as deaths and severe injuries. And then, it is normally too late for the victim because there is usually only so much that can be done in terms of investigation, courts, and so on. Another issue is that the social welfare department of the state is almost non-existent. It has become redundant in recent years, and its operation is now focused on a few issues and problems. Despite the fact that the social welfare department has shown no signs of growth or maturity in recent years, there does not seem to be any State agency that can take these cases. People are also afraid of getting involved with the police, so they are the last resort. It is our duty, as well as that of the representatives of society, to find solutions to this major issue. Abdul Rashid Hanjura, a social activist and advocate, believes that the situation in the Valley is exacerbated by the fact that many such events go unreported, resulting in no punishment for the perpetrators. Even if such incidents are identified, offenders have the audacity to continue committing crimes openly because they know no serious action can be taken against them because of the low (negligible) conviction rate.⁵²

Domestic abuse is becoming more common in Kashmir. On average, the state women's commission receives 20 domestic abuse complaints every day, and the valley's sole women's police station receives an equal number of complaints. In the valley, 2,000 cases of domestic violence were recorded last year. In the four years prior, 2,000 more people had signed up. The state women's committee, on the other hand, has already received 4,000 abuse reports this year. In the Kashmir valley, domestic violence against women is typically swept under the rug for fear of ostracisation, and the ongoing militancy and conflict has exacerbated the problem. This year, the state women's commission has received 4,000 allegations of abuse.⁵³ The continuing cycle of abuse, according to the state commission for women, is breaking women's stamina, and the majority of them simply want to escape abusive relationships. Political unrest has had such an

⁵¹ Sana, *supra* note 47.

⁵² *Id.*

⁵³ Pallavi Sharma, *Violence against women on the rise in Jammu & Kashmir*, HT, Apr. 12, 2020.

effect that women can no longer bear such events at home. They are still overburdened, so they argue that what's the point; if the relationship isn't working, it's best to quit and care for oneself.⁵⁴

Official data from Srinagar's crime division paints a bleak picture of the difficulty rape survivor's face when battling their cases in court, which can take years. According to data from the last six years (until March 2019), 1,046 rape cases are currently being tried in Jammu and Kashmir, with 831 pending since 2014. Minors are involved in about 820 of the under-trial cases. According to year-by-year data and pendency rates collected by the erstwhile state's crime division, which this author has obtained a copy of, 64 rape cases were reported in J&K in the first three months of 2019, 33 of which involved minor victims. According to the results, the conviction rate in the last six years has been less than 5%. According to a news article, the J&K administration submitted a report to the court from 2020 to April, revealing that during the lockdown period, about 16 cases of rape and 64 cases of molestation were registered in the union territory of J&K. The data reveals how crimes against women have become the rule in J&K, where they were previously considered the exception.⁵⁵

3.5 Kashmiri Women: The Worst Victims of War:

According to the records, 352 cases were reported in 2014, with 265 of them involving minors. 312 (251 minor), 263 (204 minor), and 314 (213 minor) cases were recorded in 2015, 2016 and 2017, respectively. In 2018, there were 359 rape cases recorded, with 273 of them being minor.⁵⁶

According to a report from a local news source, Indian forces have sexually abused and gang-raped over 11,000 women in illegally occupied Jammu and Kashmir over the last three decades, with another 2,342 women martyred. According to the Kashmir Media Service (KMS), Indian forces' aggression and abuse in the illegally occupied Jammu and Kashmir area has left nearly 23,000 women widowed, according to a study released earlier today in honor of the International Day for the Elimination of Violence against Women. According to the KMS, Indian troops assaulted 11,224 women during the time, citing a study by the Kashmir Media

⁵⁴ Sheikh Zafar, *In Kashmir Valley, A Sharp Rise in Domestic Violence Cases*, NDTV, Dec. 16, 2017.

⁵⁵ Sheikh, *supra* note 46.

⁵⁶ Bisma Bhat, *Collective Silence on Violence against Women Rings Loud in the Kashmir Valley*, The Wire (Jan 02, 2021), <https://thewire.in/women/collective-silence-on-violence-against-women-rings-loud-in-the-kashmir-valley>.

Service's Research Section, noting that "the Kashmiri women have been the worst victims of the harrowing war, which has left 2,923 women widowed since 1989."⁵⁷ The KMS study also highlighted how Indian troops regularly sexually harassed Kashmiri women in order to suppress the ongoing independence movement. Furthermore, over 100,000 people had mental health problems as a result of the violence committed by Indian police and troops, according to the newspaper, which cited the survey. Kashmiri politicians, according to the KMS, have repeatedly requested unbiased investigations into cases of abuse, murder, and other human rights abuses against women, such as the Kunanposhpora mass rape and the Shopian tragedy.⁵⁸

⁵⁷ *Indian Forces have raped, molested more than 11,000 Kashmiri women in 3 decades*, Geo News (Nov 25, 2020), <https://www.geo.tv/latest/320584-indian-forces-raped-molested-more-than-11000-women-in-kashmir-kms>.

⁵⁸ *Id.*

CHAPTER 4

PROTECTION OF WOMEN FROM DOMESTIC VIOLENCE

4.1 Introduction:

Domestic violence is described by the World Health Organization (WHO) as the deliberate or intentional use of any form of force, whether physical or threatening. This force may be directed at oneself or another person, or even a person's group or culture, and it could result in an injury, death, stunted growth, deprivation, or psychological damage to a human being. Domestic violence is recognized as a severe violation of human rights and a growing public health issue that has devastating consequences for a woman's emotional, physical, and sexual health. A variety of international instruments have been developed to combat violence against women. The United Nations General Assembly supported the urgent need for women's rights to freedom, protection, liberty, honesty, and dignity to be universally applied. The United Nations charter's⁵⁹ Articles 55 and 56 impose a legal duty on the organisation to uphold equality and human rights.

No one shall be tortured or subjected to cruel, inhuman, or degrading treatment or punishment.⁶⁰ Three United Nations world conferences on women have been held. The first was held in Mexico in 1975, the second in Copenhagen in 1980, and the third in Nairobi in 1985, all of which focused on developing policies to foster gender equality and opportunities for women. These were built around three goals: equality, progress, and peace. The Vienna Declaration of 1993⁶¹ calls for measures to incorporate women's human rights on an equal footing. It emphasizes the need to end violence against women in both public and private life. The Beijing Conference in 1995⁶² offered a forum for focusing on some of the main problems that had been described as major roadblocks to the progress of the majority of women around the world. It addressed problems such as gender inequality, violence against women, and so on. The “*1981 Convention on the Elimination of All Types of Discrimination against Women*” (CEDAW), which has 166 signatories, is a seminal document since it placed violence against women within

⁵⁹ United Nations, Charter of the United Nations, 24 October 1945, 1 UNTS XVI

⁶⁰ The Universal Declaration of Human Rights, 1948, art 5.

⁶¹ UN General Assembly, Vienna Declaration and Programme of Action, 12 July 1993, A/CONF.157/23.

⁶² Beijing Declaration and Platform of Action, GA Resolution 50/203, 22 December 1995.

the context of human rights. It defined women as the primary source of violence and expanded the scope of gender violence to encompass all facets of a woman's life.

The home is often compared to a haven, a place where people seek love, safety, food, and shelter. For certain people, the home is a place where lives are put in jeopardy and where some of the most heinous types of abuse against girls and women are committed. Males who are, or have been, in positions of confidence, affection, and influence, such as husbands, fathers, fathers-in-law, stepfathers, brothers, uncles, sons, or other relatives, are the most likely perpetrators of violence.⁶³

Domestic violence as described by this statute may involve a variety of forms of harassment and violence. It is any form of violence that harms you, your health, or your well-being. For dowry, money, or property, it could involve harassing or harming you or your relatives. Domestic abuse often includes the possibility of harassing or injuring others. Any act that causes you physical or mental pain is also included. Abuse can take many forms, including physical, sexual, verbal, emotional, and financial abuse. It doesn't have to be a physical act; simply not acting may be a form of domestic violence. Giving you money to run the household or for the baby, for example, will be considered economic exploitation under this act.

Domestic violence is described by the Protection of Women from Domestic Violence Act (PWDVA) of 2005⁶⁴ as any act, omission, commission, or behavior of the respondent, including threats or actual assault.

Up to 45 percent of married men admitted to sexually assaulting their wives in a 1996 survey of 6902 men in the state of Uttar Pradesh.⁶⁵ According to the National Health Survey, more than one-third of women between the ages of 15 and 49 have witnessed spousal physical abuse, according to the Ministry of Health and Family Welfare. Violence has a wide range of

⁶³ Indira Sharma, *Violence against Women: Where are the Solutions*, 57(2) Indian Journal Psychiatry 133 (2015).

⁶⁴ The Protection of Women from Domestic Violence Act, 2005, No. 43, Acts of Parliament, 2006 (India).

⁶⁵ Florence: Innocenti Digest, No 6. UNICEF Innocenti Research Centre; 2000, United Nations International Children's Emergency Fund (UNICEF), *Domestic Violence against Women and Girls, Magnitude of Problem*; pp. 4-7.

negative health effects for women, including physical, reproductive, sexual, and mental health issues.⁶⁶

In a community-based study of 450 Gujarati women, 42 percent reported physical and sexual harassment, while 23 percent reported abusive language, belittlement, and threats. It's worth noting that 56% of women believe that wife beating is justified.

According to the International Center for Research on Women (ICRW), 85 percent of men confess to engaging in abusive acts against their wives at least once in the previous 12 months. 57 percent of men confessed to abusing their wives sexually. Men confessed to abusing their pregnant wives in 32 percent of cases. To develop their dominance over the weaker sex, the men used abuse. Repeated humiliation, slurs, forced alienation; restrictions on social mobility, the persistent threat of violence and injury, and deprivation of economic opportunities are all subtle and insidious forms of violence.⁶⁷

Aggrieved person as per the law:

If you are a woman and any person with whom you are in a domestic relationship with is being abusive, you are a victim or an aggrieved person. This law aims to protect women who are living in the same house with people who are related through:

- *“Blood relationships: mother-son, father-daughter, sister-brother, widows;*
- *Marriage: husband-wife, daughter-in-law with father-in-law/ mother-in-law and other members of the family, sister-in-law with other members of the family, widows with other members of the family;*
- *Adoption - for ex. adopted daughter and father;*
- *Relationships in the nature of marriage: live-in relationships, legally invalid marriages (for e.g. husband has married a second time, husband and wife are related by blood etc.)”*

“The people need not currently be living in a shared home. For example, if the husband threw the wife out of their home, it would still be a shared home.”

⁶⁶ Florence, *supra* note 59.

⁶⁷ Washington (USA): ICRW; 2001. The International Centre for Research on Women. Domestic Violence in India II: Exploring Strategies, Promising Dialogue. ICRW Information Bulletin; pp. 1–8.

4.2 Types of Domestic Violence:

Acts of Physical Violence: Physical violence is a form of abuse that involves physical contact with the intent of instilling fear, causing discomfort, or causing other physical sufferings or bodily harm. Hitting, slapping, pulling, choking, punching, burning, and other forms of physical contact that result in physical harm to the victim are examples of physical violence.

Physical abuse often involves denial of medical treatment to a spouse or victim when it is required, depriving the person of sleep or other essential functions, and even pressuring the person to use drugs or alcohol against his or her will. In other words, if an individual is subjected to physical harm, they are subjected to physical violence.

Emotional or Psychological Abuse: Psychological violence, often known as mental abuse, may include humiliating the victim privately or publicly, limiting what the victim can and cannot do, withholding information from the victim, purposefully doing anything to make the victim feel inferior or embarrassed, isolating the victim from family and friends, and implicitly blackmailing the victim by harming others while the victim is in distress. Any type of degradation can be called psychological violence.

Emotional abuse often involves contradictory acts or comments intended to perplex and instill fear in the victim. These actions cause the survivor to doubt themselves, leading them to believe that they are fabricating their abuse or that the abuse is their fault. Women and men who are subjected to emotional violence are more likely to develop depression, which puts them at risk for suicide, eating disorders, and substance and alcohol abuse.

Sexual Violence: Any situation in which coercion or threat is used to compel others to engage in unwanted sexual behavior is considered sexual assault. Coercion of an individual to participate in sexual intercourse against their will is an act of aggression and abuse, even if the person is a spouse or intimate partner with whom consensual sex has occurred but marital rape in India is still not recognized as violence against women and there are no provisions or punishments related to marital rape in India till date. Another form of sexual assault in which a husband forces his wife to have sexual intercourse with others while allowing others to rape her which is considered as rape and is punishable by law in India and wife swapping is now considered as a crime in India.

Economic Violence: Economic exploitation occurs when one intimate partner has complete leverage over the other's access to financial services. Economic abuse may take the form of preventing a partner from acquiring resources, restricting the amount of resources available to the victim, or manipulating the victim's economic resources. The aim of preventing a spouse from gaining resources is to reduce the victim's ability to support himself or herself, causing him or her to rely financially on the offender. This involves preventing the victim from receiving education, seeking work, retaining or advancing their jobs, and acquiring properties.

4.3 Laws against Domestic Violence in India:

Currently, Section 498A of the Indian Penal Code applies if a woman is subjected to cruelty by her husband or his family. For the same, we have criminal penalties. When a married woman is subjected to cruelty by her husband or in-laws, she has the right to file a lawsuit against them. As a result, for the purposes of this section, it is critical to comprehend the definition of cruelty.

It was held in the case of *Inder Raj Malik v. Sunita Malik*⁶⁸ that the term "cruelty" is described in the explanation, which states, among other things, that harassing a woman with the intent of coercing her or any related persons to meet any unlawful demand for any property or valuable protection is cruelty. The following types of cruelty are covered in this section:

- *“Cruelty by vexatious litigation;*
- *Cruelty by deprivation and wasteful habits;*
- *Cruelty by persistent demand ;*
- *Cruelty by extra-marital relations;*
- *Harassment for non-dowry demand;*
- *Cruelty by non-acceptance of baby girl;*
- *Cruelty by false attacks on chastity;*
- *Taking away children.”*

Under this section, cruelty will be described as a serious act of cruelty that puts women in danger, and that is so serious that it can lead to suicide. It's also worth noting that in the case of

⁶⁸ *Inder Raj Malik v. Sunita Malik*, 1986 (92) CRLJ 1510 (India).

Kaliyaperumal v. State of Tamil Nadu⁶⁹, the court held that cruelty is a common element in both 304B and 498A IPC offenses. Section 304 will be discussed in greater detail in the following section of the notes.

S.498A IPC also covers any wilful behavior on the part of the husband that causes damage to the wife's "life, limb, or health (whether mental or physical)."

It is not necessary to demonstrate or prove that the woman was beaten up to prove cruelty under Explanation a) of S.498A IPC. Bullying her physically, denying her conjugal rights, or simply not listening to her properly will all come under the category of mental cruelty.⁷⁰ It is completely wrong to show some empathy to criminals or to grant them the "benefit of the doubt" when there is evidence of torture at their hands.

Domestic abuse cases are dealt with under the following provisions of the Indian Penal Code, 1860:

- *“Section 319 & 321: Hurt and voluntarily causing hurt;*
- *Section 320 & 322: Grievous hurt and voluntarily causing grievous hurt;*
- *Section 323 & 325: Punishment for causing voluntary hurt and grievous hurt;*
- *Section 349: Force;*
- *Section 350: Criminal force;*
- *Section 351: Assault;*
- *Section 503 & Section 506: Criminal intimidation and punishment for criminal intimidation;*
- *Section 307: Attempt to murder.”*

Before the 2005 Act was passed by the Parliament, there was no proper law in India to deal with civil matters of domestic abuse. In addition to the criminal remedies available to the victim in this situation, we needed legislation to address the ancillary civil issues so that the victim could receive proper relief. The framers of this Domestic Violence Act took into account

⁶⁹ Kaliyaperumal v. State of Tamil Nadu, 2004 (9) SCC 157 (India)

⁷⁰ Ramesh Dalaji Godad v. State of Gujarat, II (2004) DMC 124 (India).

Articles 14⁷¹, 15⁷², and 21⁷³ of the Indian Constitution in order to provide sufficient relief to the victims.

4.3.1 The Dowry Prohibition Act, 1961:⁷⁴

On May 1, 1961, a law was passed to prohibit the giving or receiving of a dowry. Dowry requires land, goods, or money provided by either party to the marriage, by either party's parents, or by someone else in connection with the marriage, according to the Dowry Prohibition Act. In India, the Dowry Prohibition Act extends to people of all faiths.⁷⁵

The Dowry Prohibition Act's original text was generally regarded as unsuccessful in preventing the practice of dowry. Furthermore, failure to fulfill dowry demands was still related to particular types of violence against women. As a result, the act was amended in the future. It was amended in 1984, for example, to allow gifts to be given to the bride or groom at the time of the wedding. However, the law demanded that a list be kept of each gift, its meaning, the name of the person who gave it, and the person's relationship to either of the marriage's parties. The act was also amended, as were applicable parts of the Indian Penal Code, to protect female victims of dowry-related abuse. In 2005, the Protection of Women from Domestic Violence Act added another layer of legal protection.⁷⁶

The original Dowry Prohibition Act was amended to provide minimum and maximum penalties for giving and receiving dowry, as well as a penalty for demanding dowry or advertisement money or property offers in connection with a marriage. In 1983, the Indian Penal Code was amended to include particular offences of dowry-related abuse, dowry death, and suicide abetment. When evidence of dowry demands or dowry abuse could be seen, these statutes punished violence against women by their husbands or relatives. Despite the revisions, dowry and dowry-related abuse continue to be practiced to varying degrees in India's various communities and socioeconomic classes.⁷⁷

⁷¹ Equality before Law.

⁷² Prohibition of discrimination on grounds of religion, race, caste, sex or place of birth.

⁷³ Right to Life & Personal Liberty.

⁷⁴ The Dowry Prohibition Act, 1961, No. 28, Acts of Parliament, 1961 (India).

⁷⁵ Sharmila Lodhia, *Dowry Prohibition Act (India), 1961*, Britannica (Apr 24, 2021), <https://www.britannica.com/event/Dowry-Prohibition-Act>.

⁷⁶ *Id.*

⁷⁷ *Id.*

4.3.2 Domestic Violence Act: The Legislative Dynamism:

Domestic Violence is one of the most despicable, detestable, and condemnable evils that have shaken the social conscience and it must be eradicated without delay; failing to do so will eat away at the ideals and values on which our society lived and thrived, and thus it must be eradicated. The Protection of Women from Domestic Violence Act is a laudable and glorious piece of legislation aimed at halting the tumultuous flow of violence that is destroying family mornings. In 2005, the Protection of Women from Domestic Violence Act (PWDVA) was signed into law.⁷⁸ It was only passed after extensive parliamentary debate in order to close the difference between current legal laws and the Constitution's and international human rights conventions' progressive goals.

Domestic violence victims may seek civil and criminal remedies under the Domestic Violence Act. It helps women to obtain injunctions and restraining orders, as well as penal provisions such as detention and fines, when a perpetrator violates a civil order. This more comprehensive approach to domestic violence discusses the social realities that Indian women face, such as threats of violence and psychiatric abuse, for which they often need immediate civil remedies. The Domestic Violence Act, for example, did not restrict immunity from domestic violence to married couples. The best thing about the new statute is that it has been updated to reflect current legislation. As a result, unlike past domestic violence legislation, the current Act includes "domestic partnerships," which include "all relationships focused on consanguinity, marriage, adoption, and also relationships that are "in the context of marriage."

The new law now applies to all women who are victims of domestic violence, regardless of whether the perpetrator is a spouse, domestic partner, or a live-in partner. Unmarried women, relatives, and other women living with the suspected perpetrator are also covered. For the first time, this law established the idea of "shared home," which applied to women in non-matrimonial relationships. The word "shared household"⁷⁹, may refer to a joint family property in which the male respondent is only one of several members. Also, don't forget that magistrates have the power to award monetary compensation to the victimized woman.⁸⁰ This clause guarantees that women who file lawsuits under the new law will not be evicted from their homes.

⁷⁸ *Supra* note 58.

⁷⁹ *Supra* note 58, s. 2(s).

⁸⁰ *Id.* s. 20(1).

Women were thrown out of their marital homes after filing lawsuits against their husbands, relatives, or both prior to the introduction of this new legislation. The magistrate may also issue an order granting access to the house to any woman who has thrown out after filing a case under the new legislation. To be clear, the Domestic Violence Act does not create any new criminal offenses; however, if the domestic violence case exposes any offenses punishable under the Indian Penal Code or the Dowry Prohibition Act, magistrates may file appropriate charges against the respondent and try the case themselves or refer it to the Sessions Court as necessary.

Unfortunately, there is no useful concept of "respondent" in the Domestic Violence Act. Section 2(q) simply states that "respondent" refers to an "adult male female," implying that women are not included. Several High Court decisions have interpreted this clause to include women as respondents, noting that female in-laws are often the perpetrators of domestic violence in India. By adding a proviso to this clause, the Indian Parliament eventually clarified the concept of "respondent." When the victim is a wife or woman living in a relationship in the form of marriage, the proviso includes an accused man's female relatives in the definition. This ensures that domestic violence victims will file charges against both male and female offenders.

Scope of the Act:

The constitutionality of this act has been challenged many times, but the judiciary has already established several judicial precedents that have answered many of the questions. In the case of *Krishan Lal v. Union of India*⁸¹, for example, the honorable court held that Article 14 of the Indian Constitution guarantees fair rights to all persons in similar circumstances. It was also decided that any kind of invidious discrimination is harmful to equality.

In the case of *Bhartiben Bipinbhai Tamboli v. State of Gujarat*⁸², the scope of the Act was addressed. Domestic abuse is rampant in India, according to the court in this case. Every day, as a daughter, mother, wife, sister, partner, or single woman, many women face it in some form or another. Despite this, it is the least recorded type of cruelty, owing to social stigma and women's attitudes.

The remedies available to a survivor of domestic abuse were very minimal until 2005. They must either file for divorce in civil court or prosecute the offence under Section 498-A of

⁸¹ *Krishan Lal v. Union of India*, 1994 CriLJ 3472.

⁸² *Bhartiben Bipinbhai Tamboli v. State of Gujarat*, MANU/GJ/0025/2018.

the Indian Penal Code in criminal court (cruelty by the husband or his relative). Relationships that were not married were also not recognized. Such factors compelled a woman to remain silent. The Protection of Women from Domestic Violence Act of 2005 was passed in response to all of this. The concept of an aggrieved individual in this Act is very broad (it includes women in live-in relationships) and it seeks to protect a woman from abuse perpetrated by a man and/or a woman.

As a result, the Act has a broad scope and affects a vast number of women who previously had few options. Women's Protection from Domestic Violence the Women's Rights Act of 2005 was enacted to provide adequate safeguards for women's rights guaranteed by our constitution, with an emphasis on women who have been victims of domestic violence and other incidental matters.

The following are the Act's key provisions:

- “Under this Act, the victim does not have to file a complaint about domestic violence; instead, any person who has a reason to believe that such an act has been or is being committed by a person may file a complaint. Thus, it allows neighbors, relatives, other family members, and numerous social workers the right to file a complaint; moreover, it must be shown that the complaint is filed in good faith;
- The magistrate has been given the authority to allow the victim to remain in her adobe home and to prevent the male relatives from evicting her. The Magistrate may also issue orders allocating a portion of the house to the victim for her personal use;
- The Magistrate may issue orders under Section 18 of the Act prohibiting the respondent from contacting the aggrieved woman by any means of communication so that she is not intimidated in any way. In addition, the respondent's access to her office, her home, her child's education, and other places can be refused;
- According to Section 22 of the Act, the respondent may be required to compensate for the costs and damages incurred by the respondent's injury, which may include mental torture and emotional distress. If the victim has lost earnings as a result of the incident or injury, the victim may be entitled to compensation. In addition, the respondent may be held liable for any damage to the land;

- The Act stipulates a sentence of up to one year in jail or a fine of Rs. 20,000 for such an act. The act also states that any offense committed under it is punishable by law and is not bailable. Furthermore, the court may conclude that the crime was committed by the accused based solely on the evidence of the aggrieved party;
- The Act has since ensured that victims of domestic abuse receive prompt justice. The hearing must be held within three days of the complaint being filed, and each case must be resolved within 60 days of the first hearing;
- The Act also requires states to have security agents, medical facilities, and service providers in accordance with the requirements;
- The Magistrate has the authority under Section 16 of the Act to keep the trial in camera if the case needs it or if the victim or the respondent requests it;
- In addition to the above provisions, the Act also includes protection orders under section 18, residence orders under section 19, monetary reliefs under section 20, custody orders under section 21, and reimbursement orders under section 22.”

Effects on Victims & their Children’s:

Survivors of domestic abuse also suffer from a variety of psychosomatic conditions, eating disorders, insomnia, stomach disturbances, generalized chronic pain, and debilitating mental health issues such as Post-traumatic Stress Disorder (PTSD). Long-term and short-term physical and mental health problems may also be caused by violence. Asthma, chronic pain, heart disease, migraine headaches, and other long-term health issues are examples. To deal with these issues, some women resort to risky behaviors such as having unsafe sex, abusing alcohol, or abusing narcotics. It also alters a person's view of his or her own body. Minor injuries that can be observed by scans or x-rays are examples of short-term physical effects. Bruises, burns, organ damage, and other types of injuries are among them.

Emotional and psychological trauma involves things like rage, guilt, and suicide, which can have a detrimental effect on a person's personality. Shame and humiliation can be a factor that prevents an individual from seeking out aids or resources that can assist them in dealing with such issues. Fear, anxiety, frustration, depression, social isolation, and even suicidal ideation are all exacerbated by a lack of emotional support. These wounds last for years and are often left untreated because they are not visible on x-rays.

Economic homelessness is the most effective way for survivors of domestic abuse to protect themselves from the violent nature of their relationship. In 2017, homelessness services agencies set aside more than 55,000 beds for survivors of domestic abuse on a single night. About 31,500 adults and children fleeing domestic violence sought refuge in an emergency shelter or transitional housing program on a single day in 2015. Due to a lack of support, manpower, or other tools, domestic violence programs were unable to fulfill over 12,197 demands for services on that day.

When victims leave the accused, they can be taken aback by the fact of how much power the violence has taken away from them. Because of the economic violence, the victim typically has very little money and few people to turn to for assistance. This has been shown to be one of the most difficult obstacles for victims of domestic abuse, as well as the most powerful factor that can deter them from leaving the perpetrator.

According to studies, more than half of female survivors have children in their care. Domestic abuse can harm children in a variety of ways, including the development of phobias or insomnia, stress management, difficulty establishing healthy relationships with others, and physical symptoms such as headaches. Children need a safe atmosphere in which to grow up. They do not feel comfortable in a home where domestic abuse occurs. Children who experience such violence may become victims themselves. These kids are at a high risk of developing long-term physical and mental health problems. Mental health issues, such as depression, are examples of this. The age factor plays a role in the disruption caused by violence.

Small children are among the most vulnerable victims of such abuse. Many that are not directly harmed have some of the same behavioral and psychological issues as physically abused children. These children may struggle to learn new things and may be depressed or anxious. Younger children are more vulnerable, and it is distressing that abuse is more common in households with small children. As a result, there's a chance that this will perpetuate the cycle of abuse for the next generation. There is also a substantial risk that their physical, mental, and social growth may be harmed more in the future.

Children in age group of 14 - 20 may feel responsible for the violence and blame themselves for it. They might not be able to study effectively and achieve good grades. It's also

possible that they won't engage in extracurricular sports. Due to the problems, they may feel less fortunate and have fewer friends than a typical child.

Teens who experience violence can exhibit negative behaviors such as developing bad habits, fighting with others, and failing to understand others' viewpoints. One in every six (16%) college women has experienced verbal harassment by a dating partner. This brutality, however, can be avoided. A consortium of ten international organisations, led by the World Health Organization, have created and endorsed INSPIRE: Seven strategies for ending violence against children, an evidence-based technical kit.

This aims to assist countries and communities in achieving SDG Goal 16.2 on ending child abuse. Every letter of the word INSPIRE represents one of the interventions, and the majority of them have been shown to have protective effects on a variety of forms of abuse, as well as benefits in areas like mental health, education, and crime prevention. The following are the seven strategies:

- *“Implementation and enforcement of laws;*
- *Norms and value change;*
- *Safe environment;*
- *Parental and caregiver support;*
- *Income and economic strengthening;*
- *Response services provisions;*
- *Education and life skills.”*

Effects on Community:

Domestic abuse has an effect not only on the family, but also on the community, as children grow up without knowing how to form healthy and respectful relationships with others. Domestic abuse has a devastating effect on societies and communities. Its societal cost is enormous, and the following are some of the consequences of domestic abuse.

The government's healthcare subsidy is in jeopardy: The government's position in addressing health equity is critical. India's public health system is guided by the Ministry of Health and Family Welfare (MOHFW). The government has strained medical care due to a rise

in the number of domestic abuse incidents. The total cost of medical treatment for injuries caused by domestic abuse has surpassed \$44 million.

Economic ramifications: Another economic ramification of this exploitation is the loss of long-term productivity that businesses face. The majority of the victims fail to turn up at work, which has a negative impact on productivity. This consideration is one of the reasons why several businesses have implemented measures that counter domestic abuse. They are looking for ways to communicate with agencies in order to offer protection to their employees. They're attempting to provide a healthy working atmosphere for them, which is beneficial to society.

Possible Misuses of Domestic Violence Act:

The Domestic Violence Act of 2005 was enacted by the legislature to protect women from abuse of any sort, and a great deal of emphasis was placed on this. Sadly, little attention was given to the fact that men may also be victims of harassment, and the time has come to reconsider the issue of male protection from the hands of women. The Hon'ble Supreme Court held in the case of *Dr. N. G. Dastane v. Mrs. S. Dastane*⁸³ that cruelty can be of two types: emotional and physical. While it is true that physical abuse is always perpetuated by a powerful husband, this cannot be said to be universally true. In the case of mental cruelty, it's even the other way around. However, in the vast majority of cases of mental torture, it is almost always the wife who is the perpetrator.

Furthermore, in the case of *Sushil Kumar Sharma v. Union of India*⁸⁴, the Supreme Court of India stated that by misusing the clause, a New Legal Terrorism can be unleashed. Now comes the question of whether laws enacted to protect women can be abused. In response to this issue, the Honorable Supreme Court stated in a case that unfortunately, a large number of these grievances have not only overwhelmed the courts but have also contributed to immense social turmoil, affecting the society's stability, harmony, and happiness. The Supreme Court made this finding in relation to the Domestic Violence Act. It's important to remember that the term cruelty does not apply solely to women. Men may also be victims of this, and cruelty or violence does not always have to be physical; in some situations, it can also be emotional. Victimization of male partners, as well as police harassment, is a major issue in these situations. The Act has often

⁸³ *Dr. N. G. Dastane v. Mrs. S. Dastane*, AIR 1975 SC 1534.

⁸⁴ *Sushil Kumar Sharma v. Union of India*, A.I.R. 2005 S.C. 3100

been chastised for its ambiguity and lack of clarification. Explanation I (iii) of Section 3 of the Act, for example, contains insults and jibes in the concept of physical and emotional violence, without specifying these words. As a result, the term mental and verbal assault has the potential to be misconstrued. It may be applied to simple domestic disputes that were not meant to come under the scope of mental and verbal violence in some situations. It's worth noting that, sadly, the aggrieved party in the Domestic Violence Act of 2005 is always any woman. Such a description does not include the term guy. As a result, the Act only applies to women who have been aggrieved. Even the preamble mentions women's rights. According to the standard, a respondent is any adult male person, which means a complaint cannot be aimed at a woman. When we think that a female partner in a live-in relationship that may have only lasted a month can demand maintenance allowance under this clause with no limitations, we can see how provisions like section 20(1) (d) can be abused.

Loopholes in the Present Domestic Violence Act, 2005:

Whenever a bill relevant to some subject is introduced in Parliament, it is done so with the society's future needs in mind. The Indian Penal Code, 1860, is one of the best examples of such a statute. It was drafted more than a century ago, but it is still relevant in Indian society. Despite the fact that certain changes have been made to the Act, it has not lost its applicability or impact.

When the Domestic Violence Act was drafted and passed, it was regarded as one of the most progressive laws in Indian history because it provided many solutions to victims of domestic violence, as well as acknowledging and addressing the related issues. One of the most striking aspects of this Act is that it implicitly tackles live-in partnerships while also protecting victims of domestic abuse. However, due to rapid societal change, the Act gradually created several loopholes. The following are some of the most common criticisms leveled at this Act:

- “There is a lack of evaluation and monitoring of the shortcomings and successes of pro-women legislation because states have been granted the responsibility to do so, but they refuse to do so;
- Although the Act provides several solutions for women, it fails to resolve the abuse that men face in society. Men may be victims as well, but some see it as a psychological

illness, while others see it as a source of ridicule, with a lack of male chauvinism and dominance over their wives causing shame for such men. Domestic violence is not limited to one individual or gender, and lawmakers have failed to address this issue;

- This Act has been abused on many occasions. When marriages become sour, women use this Act as a tactic to threaten the husband's life and make their lives as miserable as possible. Lawyers have also been misinforming their clients about filing a lawsuit under this Act in order to strengthen their claims and earn a large sum of money through compensations;
- The authorities included in the Act have also consistently failed to provide sufficient relief to the victims. They are imbued with patriarchal social norms, making them unable to consider such grievances and take any action seriously. In such a case, the woman is often given a compromise. The security officers needed by the Act are not fully employed for this role, and it is often assigned as an extra duty to already employed government employees, who, in turn, do not take the cases seriously;
- Domestic abuse can be a recurring offense for many victims of society, and late case resolution has resulted in many deaths. Though the Act requires cases to be resolved within 60 days, this is rarely the case, and often cases remain unresolved for years, making the lives of both the victim and the respondent more difficult;
- The act empowers everyone, regardless of whether or not she is a survivor, to file a lawsuit against it. This has resulted in many people abusing the law and filing false charges with no proof in order to exact vengeance on others;
- Under section 32(2) of the Act, the court may find that the respondent committed an offence based solely on the evidence of the victim, which has often been used by women to settle their scores with their husbands or his relatives;
- There is still a dearth of instruction for Magistrates and police officers in relation to the Act. Officers lack the empathy needed for this situation, and they do not follow the Act's requirements. As a result, women have been re-victimized by the criminal justice system. In the case of women, police officers are still not very sensitive to this crime, which may lead to trauma;
- The efforts of non-governmental organizations (NGOs) as service providers are waning as they are unable to deal with the problem without the adequate help of other authorities;

- In addition to the above flaws, there are other problems such as the dual system of family and criminal courts, which makes redress more difficult, inequalities in enforcement across states, public resistance due to inadequate redress mechanisms, and failure to meet the criminal penalties mandate.”

Important Case Laws:

Sandhya Wankhede v. Manoj Bhimrao Wankhede⁸⁵: The term "respondent" is described in Section 2(q) of the Domestic Violence Act as any adult male who is, or has been, in a domestic relationship with the aggrieved person and against whom the aggrieved person has sought any relief under this Act: Provided, however, that an aggrieved wife or female living in a marriage-like relationship might also file a lawsuit against a husband's or male partner's parent. Since the term respondent is defined to include an adult male person, the judiciary has been faced with the contention that an aggrieved person can only file a complaint under the Domestic Violence Act against an adult male person and not against the husband's female relatives, such as his mother-in-law or sister-in-law. However, in the above case, the Supreme Court decided that the proviso to Section 2(q) does not preclude female relatives of the husband or male partner from the scope of a complaint that can be filed under the Domestic Violence Act. As a result, charges may be filed not only against an adult male but also against a female spouse of that adult male.

Sabita Mark Burges v. Mark Lionel Burges⁸⁶: Domestic Violence Act Section 19(1)(b) allows an order to be issued ordering the Respondent to leave the shared household. As a result, the Magistrate has the authority to issue an order ordering the respondent to leave the shared household. In this case, the Bombay High Court held that regardless of whether a man is the sole owner of a home, he has no right to be violent against his wife or the woman with whom he resides, and that if the Court witnesses such abuse, he must be barred from entering the residence, effectively to protect the wife and children from further violence and similar disputes. It is common knowledge that claims for injunctions in respect of the respondent's residence and ownership are seen by courts as primarily affecting the parties' proprietary rights. Since most wives do not own matrimonial homes, they are granted statutorily granted privileges that would

⁸⁵ Sandhya Wankhede v. Manoj Bhimrao Wankhede, 2011 (3) SCC 650.

⁸⁶ Sabita Mark Burges v. Mark Lionel Burges, 2013 SCC Online Bom 631.

not have been granted by courts under common law principles, such as the right to peaceful enjoyment of their matrimonial home. In the first place, Section 19 of the Domestic Violence Act was passed, granting effectively the wives/women peace against domestic violence in their homes, regardless of their names. The sublime concept of human rights prevailing over proprietary rights underpins this constitutional grant. It is worth repeating that unless one of them is abusive, they are both equally entitled to the said flat.

Meenavathi v. Senthamarai Selvi⁸⁷: The proviso to Section 19 of the Domestic Violence Act clearly states that no order under Section 19 (1) (b) of the Act can be issued against a woman. It was held in this case that such women members of the family cannot be ordered to be excluded from the joint household under the guise of passing an order under Section 19 (1) (b) of the Domestic Violence Act. The High Court of Madras made a similar observation in the case of *Uma Narayanan v. Mrs. Priya Krishna Prasad*⁸⁸, where the Court stated that the Magistrate is empowered to issue an order ordering the respondent to withdraw himself from the shared household under Section 19 (1) (b) of the Domestic Violence Act. The said proviso has been added only to protect the interests of a woman member of the family who is living in such a joint household while enumerating the directions that can be passed under Section 19 (1) (b) of the Domestic Violence Act and with specific reference to the direction that can be given under Section 19 (1) (b) of the Domestic Violence Act. The proviso contains a clause like this only for the above restricted reason. Women members of the family may live in a shared household that belongs to a joint family, and such women members of the family cannot be ordered to leave the shared household under the guise of passing an order under Section 19(1) (b) of the Act, but such a direction can be given only against male members.

V.D. Bhanot v. Savita Bhanot⁸⁹: In this case, the Supreme Court upheld the Delhi High Court's decision that "even a wife who shared a household before the Domestic Violence Act came into force would be entitled to the Domestic Violence Act's defense." As a result, the Domestic Violence Act allows an aggrieved party to file an application under the Act for actions committed before the Act's inception.

⁸⁷ *Meenavathi v. Senthamarai Selvi*, CRL OP (Md.) No. 12092 of 2008.

⁸⁸ *Uma Narayanan v. Mrs. Priya Krishna Prasad*, Criminal Original Petition No. 9277 of 2008.

⁸⁹ *V.D. Bhanot v. Savita Bhanot*, MANU/SC/0115/2012.

Mohd. Zakir v. Shabana & Ors⁹⁰: In this fascinating case from 2018, the High Court of Karnataka ruled that a petition filed by the husband or an adult male under the Domestic Violence Act may be heard. The High Court based its decision on the Supreme Court's decision in Hiral P. Harsora v. Kusum Narottamdas Harsora⁹¹, in which the Supreme Court struck down a portion of Section 2 (a) of the Act (defining aggrieved person) on the grounds that it is in violation of Article 14 of the Indian Constitution, as well as the phrase adult male as found in Section 2(q) of the Act. In light of the aforementioned Apex Court ruling, the High Court opined that if the said sub-section is read without the term adult male, it appears that any individual, male or female, who is aggrieved and alleges a violation of the Act's provisions, could invoke the Act's provisions. In that light, the petitioner's case should not have been dismissed on the grounds that the Act does not provide for men and that it is only applicable to women. However, Justice Anand Byrareddy later withdrew the aforementioned High Court judgement after an Advocate objected to it, arguing that the Supreme Court's verdict in the Hiral Harsora case had been incorrectly interpreted by the Judge.

Indra Sharma v. V.K.V. Sharma⁹²: The Supreme Court ruled in this case that not all live-in partnerships are marriage-like relationships. Guidelines for putting the live-in-relationship principle to the test:

- *“Relationship period;*
- *Household that is shared;*
- *Services and financial plans are pooled;*
- *Domestic situations;*
- *Intention and behavior of the parties in sexual partnership Children's socialization in public.”*

Lalita Toppo v State of Jharkhand⁹³: In this case, the court claimed unequivocally that an estranged wife or someone in a live-in relationship who is not legally married is entitled to maintenance under the Act, not Section 125 of the CrPC. The court interpreted Section 3(a) broadly, including economic coercion as a form of domestic violence.

⁹⁰ Mohd. Zakir v. Shabana & Ors, Criminal Appeal No. 926 of 2018.

⁹¹ Hiral P. Harsora v. Kusum Narottamdas Harsora, Civil Appeal No. 10084 of 2016.

⁹² Indra Sharma v. V.K.V. Sharma, Criminal Appeal No. 2009 of 2013.

⁹³ Lalita Toppo v State of Jharkhand and Ors, MANU/SC/1476/2018.

Is there an obligation on husband to maintain their wife under the Act?

The court held in *Vimla Ajitbhai Patel v. Vatslaben Ashokbhai Patel*⁹⁴ that the Domestic Violence Act must be read in conjunction with the Hindu Adoption and Maintenance Act, 1956. As a result, husbands have a personal responsibility to help their spouses.

In *Binita Dass v. Uttam Kumar*⁹⁵, the court explained that qualification and earning ability cannot be used to deny interim maintenance to the wife.

Furthermore, in *Smt. Haimanti Mal v. State of West Bengal*⁹⁶, the Calcutta High Court held that such compensation should not be based on guesswork but rather on some reasonable basis. Also, as in *Manju Sharma v. Vipin*⁹⁷, when the husband tries to display less income in order to offer less money, proper identification must be done and adequate and proportionate maintenance must be given.

Even if the wife is well qualified, the Supreme Court recently held in *Megha Khandelwal v. Rajat Khandelwal*⁹⁸ that the husband has a duty to pay maintenance to her.

In *Krishna Bhattacharjee v. Sarathi Choudhary*⁹⁹, the Supreme Court issued some guidelines. It was decided that:

- It is the court's responsibility to examine all of the facts to see whether they are legally sound, and the court must not be biased in doing so;
- The theory that "justice to the cause is equal to ocean salt" should be considered, and the facts should be upheld in order to impart justice;
- Before dismissing a lawsuit, the court must determine if the aggrieved individual under the statute has been subjected to non-adjudication, as the act is designed to benefit women in society and uphold constitutional values.

⁹⁴ *Vimla Ajitbhai Patel v. Vatslaben Ashokbhai Patel and Ors*, 2008 (4) SCC 649.

⁹⁵ *Binita Dass v. Uttam Kumar*, MANU/DE/2870/2019.

⁹⁶ *Smt. Haimanti Mal v. State of West Bengal*, C.R.R. 3907 of 2016.

⁹⁷ *Manju Sharma v. Vipin*, MANU/DE/2061/2019

⁹⁸ *Megha Khandelwal v. Rajat Khandelwal*, MANU/SCOR/16958/2019.

⁹⁹ *Krishna Bhattacharjee v. Sarathi Choudhary and Another*, 2016 (2) SCC 705.

Duty of wife not to implicate all members of the family: The court held in *Ashish Dixit v. State of U.P.*¹⁰⁰ that a wife cannot implicate anyone in the family other than her husband and in laws, as in the present case, the plaintiff made even those members a party to the suit, even though the claimant was unaware of their names.

Domestic Violence during 2020 Pandemic:

With the dramatic rise in COVID-19 cases around the world in recent months, some international organisations have noticed a global spike in Domestic Violence (DV) cases as a result of physical distancing laws and the resulting lockdowns. The number of distress calls received from women confined in closed spaces with violent partners increased by 15-30% in many countries. Studies have shown a strong correlation between periods of crisis and interpersonal conflict over the years. Pandemics create a fearful and unpredictable atmosphere that can intensify various types of violence against women. Furthermore, economic inequality, financial uncertainty, and alienation are all factors that lead to the spread of domestic violence. Domestic violence cases are unfortunately underreported all over the world, particularly during global emergencies like COVID-19.¹⁰¹

Domestic abuse perpetrator's grip has tightened in India during the pandemic. Victims of abuse are cut off from their usual support networks, making it impossible for them to seek help. The Prime Minister of India declared a national lockdown on March 24, 2020, in order to stop the spread of the Novel Coronavirus. The National Commission on Women (NCW) registered a 100 percent increase in domestic violence reports within a fortnight. The NCW then introduced a national WhatsApp number to provide an alternative way for women to report domestic violence.

While there was an obvious increase in the number of domestic violence cases in India at the time, the NCW monthly data revealed a different story. In contrast to even the first months of 2020, there was an overall decline in the number of complaints received during the months of lockdown (Complaints received: January: 538, February: 523, March: 501, April: 377). However, as the lockdown was gradually lifted, the number of complaints increased. In May,

¹⁰⁰ *Ashish Dixit v. State of U.P and Another*, (2013) 4 SCC 176.

¹⁰¹ Kanika Arora & Shubham Kumar, *Locked-Down: Domestic Violence Reporting in India during Covid-19*, OXFAM India (Aug 03, 2020), <https://www.oxfamindia.org/blog/locked-down-domestic-violence-reporting-india-during-covid-19>.

there were 552 complaints, but in June, there were more than 730. Although there was a legitimate concern about an uptick in domestic violence cases during the lockdown, this data indicates that the incidents were not actively publicized.

An examination of cases recorded across the country by the Hindustan Times reveals two key aspects of the issue. One, while some states have seen a decrease in the number of domestic abuse complaints, others have seen an increase in the number of calls to helplines. This suggests that the willingness of victims to make allegations when sharing domestic spaces with offenders affects the rate of domestic violence during the lockdown. The number of complaints received by state-run helplines has decreased in some states, such as Rajasthan, Madhya Pradesh, and Telangana. Domestic violence incidents decreased by around 50% in Ghaziabad, which is part of the National Capital Region, during the first phase of the lockdown, compared to the pre-lockdown period in March, according to data collected by 18 police stations in the city's urban and rural areas. The second part of this problem is that, while there are many helplines and shelter homes for women to call or live in — both state-run and non-governmental — the assistance that they can offer has been limited due to the lockdown. Women are unable to drive to police stations, and social workers are unable to contact them or arrange for their transportation; police officers are overburdened with Covid-19 responsibilities, and visiting homes to investigate domestic disputes is often not a priority. Domestic abuse lawsuits are also filed in lower courts because they are civil disputes, and courts are only available for emergency trials, such as bail pleas, at the moment.¹⁰²

Reporting barriers in the midst of a pandemic:

In India, a series of COVID-19 lockdowns hampered the ability to register domestic violence incidents which are discussed below:

Restricted movement: The lockdown rendered women helpless by prohibiting them from fleeing violent or abusive situations. Women's privacy was eroded as men and women cohabitated for longer periods of time, and incidents of abuse increased.

¹⁰² Kanika, *supra* note 95.

Limited access to communication: The NCW's WhatsApp number had a limited scope since only 38% of Indian women own phones and even fewer have access to the internet, rendering this platform unavailable to the majority of women in the world.

Less contact with natal kin: The victim's natal family is normally the first point of contact. They are not only necessary for assisting the victim in filing a lawsuit, but they also make filing complaints with the police easier. Victims found it impossible to reach their first responder due to the perpetrator's relentless presence, which discouraged them from reporting to institutionalized networks.

Lack of formal support: During the lockdown, the machinery established under the Protection of Women from Domestic Violence Act was not identified as an important service. As a result, security officers were unable to visit victims' homes, NGOs were unable to provide physical contact with them, and police officers, who were at the forefront of our effort to combat COVID-19, were overworked and unable to adequately assist victims.

Although national controls have been eased, lockdowns at the state and district levels are still used on occasion, allowing a pandemic of domestic violence to spread. We must not accept violence against women as an unavoidable consequence of a crisis, but rather strengthen the otherwise postponed policy consequences to fix the issue.

CHAPTER 5

MEASURES TAKEN BY THE INDIAN LEGISLATURE AND JUDICIARY TO CURB VIOLENCE AGAINST WOMEN

5.1 Introduction

Throughout the years, the judiciary's intervention has been liberal and democratic. Judicial advocacy, which is on the rise, has been extremely beneficial to women's security and empowerment. Since the judiciary cannot make legislation but can only interpret and pass decisions on it, its attention to women's protection is admirable. But that doesn't change the fact that robberies, kidnappings, killings, and dowry deaths have all increased significantly this year. Data from the National Crime Records Bureau indicates a 12-15 percent increase in rape, as well as other crimes against women. If it weren't for the pending litigation and the time it takes for judgments to be delivered, the country and women's protection would advance more quickly. Women in India have long been marginalized, but things have improved since the establishment of the judiciary, but not to the level that they should be. To deter offenders from committing more heinous crimes, the penalties should be more severe. This paper will examine the involvement of the judiciary in the prevention of crimes against women in depth, citing key cases in the process. It will also make recommendations for accelerating the delivery of judgments and the establishment of justice in the country. Article 21 of the Indian Constitution guarantees all the right to life, and the crime rates we know are only based on confirmed cases. There are several rapes and murders of women that go unreported. There is enough regulation in place, but it is not being implemented properly. The pressing issue is not so much a fight against a specific oppressor as it is a fight against a collection of values that pervades society. This paper examines the different causes of violence against women in our country, as well as the various laws in place and their applicability to women's defense in our country. This paper examines the judicial attitude toward crime against women in depth and sheds light on recent developments in judicial sensitivity to crime against women.

5.2 Special Laws:

While all laws are not gender specific, the provisions of law affecting women considerably have been reviewed from time to time and amendments were made to keep pace

with the evolving society. The following laws are having special provisions to protect women and their safety:

- “Indecent Representation of Women (Prohibition) Act, 1986;
- The Immoral Traffic (Prevention) Act 1986;
- Dowry Prohibition Act, 1961;
- Commission of Sati (Prevention) Act, 1987;
- The Protection of Women from Domestic Violence Act, 2005;
- Information Technology Act 2000;
- The Sexual Harassment of Woman at Workplace (Prevention, Prohibition and Redressal) Act, 2013;
- The Prevention and Protection from Witch Hunting;
- Pre-Conception & Pre-Natal Diagnostic Techniques Act, 1994;
- The Medical Termination of Pregnancy Act, 1971;
- The Prohibition of Child Marriage Act, 2006.”

In an incident that shakes the country on 16 December 2012 where a female student intern was beaten and gang raped in Delhi and after few days later in spite of receiving medical treatment, the victim was no longer alive. The incident led to condemnation by the United Nations and other International women organizations, and called upon government of India to do everything in their power to take up radical reforms, ensure justice and reach out with robust public services to make women’s lives more safe and secure.

Against the backdrop of the nation-wide outrage over the tragic Delhi gang-rape, Nirbhaya (Fearless) incident of December 16, 2012, propelled the Government of India (GOI) to drive the issue of violence against women to the centre-stage of political discourse. Consequently, on December 22, 2012, GOI appointed a three-member judicial committee headed by the former Chief Justice of India, Justice J.S. Verma. The key objective of the Commission was to review for possible amendments to the criminal law and suggest measures for faster trials and strict penalties for brutal offences related to crime against women. Taking further cognizance of the strident storm of public protests in general and a tribute to Nirbhaya (Fearless) in particular, on January 23, 2013, the commission submitted its recommendations by identifying

lack of good governance as the central cause of violence against women. The commission goes on to criticize the government, the abysmal and old-fashioned police system alongside public apathy in tackling violence against women, and thereby, recommends dramatic transformation in legislations. The recommendations are based on more than 80,000 suggestions received from stakeholders, social activists and public comprising eminent jurists, legal professionals, NGOs, women's groups and civil society through varied methods: emails, posts and fax. A 631-page report consisting of 14 chapters include recommendations on laws related to rape, sexual harassment, trafficking, child sexual abuse, medical examination of victims, police, electoral and educational reforms. Based on some of the recommendations of the Justice Verma Committee (JVC) report, an anti-rape Ordinance was enacted and signed by the Honorable President of India, Mr. Pranab Mukherjee on February 03, 2013. The Criminal Law (Amendment) Bill, 2013, passed in the parliament.

5.3 Changes brought in Criminal Law by the Criminal Law (Amendment) Act, 2013:

The Nirbhaya Case:

The victim, a 23 year old woman and her boyfriend, were on their way home on the night after watching a film in Saket, South Delhi they entered an off-duty private bus at Munirka for Dwarka that was being driven by joyriders at about 9:30 pm at night. There were only six persons on the bus, including the driver. The woman's friend became suspicious when the bus deviated from its normal route and its doors were locked. When he objected, all the six men, including the driver, taunt the pair. When the woman's boyfriend attempted to interfere, he was restrained, and beaten unconscious with an iron bar. The men then pulled the woman to the back of the bus, beating her with the bar and raping her whereas the bus driver continued to drive. As per the police information the woman try to fight her assailants, biting three of the assailants and leaving bite marks on the accused men. After thrashing and raping, the assailants threw both victims from the moving bus. After that the bus driver purportedly attempted to drive the bus over the woman, but she was pulled aside by her boyfriend. One of the perpetrators afterward cleans the vehicle to get rid of proof. The partially clad wounded were found on the road by a person walking by at around 11 pm at night. The passerby phoned the Delhi Police, who took the duo to Safdarjung Hospital, where the woman was given emergency medical aid and placed on Ventilation. The woman victim has injury marks, including many bite marks, all over her body.

In compliance with Indian law, the real name of the victim was initially not released to the media, so pseudonyms were used for her by various media houses instead, including Jagruti (awareness), Jyoti (flame), Amanat (treasure), Nirbhaya (fearless one), Damini (lightning, after the 1993 Hindi film) and Delhi Braveheart. The friend of Nirbhaya who was attacked, suffered broken limbs but survived. On 19 December 2012, the woman underwent her fifth surgery, removing most of her remaining intestine. On 21 December, the government appointed a committee of physicians to ensure she received the best medical care. By 25 December, she remained incubated, on life support and in critical condition. At a cabinet meeting chaired by Prime Minister Dr. Manmohan Singh on 26 December, the decision was made to fly her to Mount Elizabeth Hospital in Singapore for further care. Mount Elizabeth is a multiorgan transplant specialty hospital. On 28 December, at 11 am, her condition was extremely critical. The chief executive officer of the Mount Elizabeth Hospital said that the woman suffered brain damage, pneumonia, and abdominal infection, and that she was fighting for her life. Her condition continued to deteriorate, and she died at 4:45 am on 29 December, Singapore Standard Time. Her body was cremated on 30 December in Delhi under high police security.

Effects of Nirbhaya Case:

Public protests took place in New Delhi on 21 December 2012 at India Gate and Raisina Hill; Thousands of protesters clashed with police and battled Rapid Action Force units. Demonstrators were lathi charged, shot with water cannon and tear gas shells, and arrested. Alike protests occurred throughout the country. Huge number of women belonging to various NGO's and other organizations demonstrated in all parts of the country. Protests occurred online as well on the social networking sites Face book and WhatsApp, with users replacing their profile images with a black dot symbol. Tens of thousands signed an online petition protesting the incident. this led to The Government of India has set up Justice Verma Committee to recommend amendments to the Criminal Law so as to provide for quicker trial and enhanced punishment for criminals of committing sexual assault against women after the Nirbhaya incident. The Committee headed by J. S. Verma, a former Chief Justice of India and one of India's most highly regarded Chief Justices and eminent jurists submitted its report on January 23, 2013. It made recommendations on laws related to rape, sexual harassment, trafficking, and child sexual abuse, medical examination of victims, police, electoral and educational reforms.

After the Nirbhaya incident, Govt. of India has enacted the Criminal Law (Amendment Act), 2013¹⁰³, to redefine the sexual crimes against women. It provides for amendment of the Indian Penal Code, Indian Evidence Act, and Code of Criminal Procedure, 1973. The crime of rape has been altogether redefined and to say the least this definition and inclusion of some other acts of sexual nature against women in the offence of rape is a new era of criminal jurisprudence.

The changes that have been brought about by the criminal law amendments are the incorporation of new offenses in the Indian Penal Code, which are enumerated below:

Section 326A:¹⁰⁴ *“A gender neutral provision, provides for the penalties for acid attacks as imprisonment of not less than ten years but which may extend to imprisonment for life and with fine which shall be just and reasonable to meet the medical expenses and it shall be paid to the victim.”*

Section 326B:¹⁰⁵ *“A gender neutral provision provides for penalties for engaging in an attempt to attack with acid and gives for imprisonment of not less than five years but which may extend to seven years, and shall also be liable to fine. The explanation to the section also provides for inclusion of all substances that have a corrosive, burning or acidic nature. Also it further provides that such an attack need not have any irreversible section for the section to apply.”*

Section 354A:¹⁰⁶ *“provides for penalties for the offense of sexual harassment. It provides for rigorous imprisonment up to three years, or with fine, or with both for events described in clauses (i) & (ii), imprisonment up to one year, or with fine, or with both in other cases (i) Physical contact and advances involving unwelcome and explicit sexual overtures; (ii) A demand or request for sexual favors; or (iii) Forcibly showing pornography; or (iv) Making sexually colored remarks”*

¹⁰³ Criminal Law (Amendment Act), 2013, No. 13, Acts of Parliament, 2013 (India).

¹⁰⁴ *Id.* s. 5

¹⁰⁵ *Id.*

¹⁰⁶ *Id.* s. 7

Section 354B: *“It provides for imprisonment of not less than three years but which may extend to seven years and with fine for assaults or use of criminal force on any woman or for abetment of such an act with the intention of disrobing or compelling her to be naked.”*

Section 354C:¹⁰⁷ *“It includes a new offense of Voyeurism. In case of first conviction for this offense, imprisonment not less than one year, but which may extend to three years, fine. In the event of second or subsequent conviction, a punishment of imprisonment for a term which shall not be less than three years, but which may extend to seven years, and shall also be liable to fine. In defining the offense of voyeurism, the act provides that watching or capturing a woman in a private act, includes an act of watching carried out in a place which, in the circumstances, would reasonably be expected to provide privacy, and where the victim’s genitals, buttocks or breasts are exposed or covered only in underwear; or the victim is using a lavatory; or the person is doing a sexual act that is not of a kind ordinarily done in public.”*

Section 354D:¹⁰⁸ *“It introduces another new offense of Stalking, This section provides for an Imprisonment of not less than one year but which may extend to three years, and fine. This section can only be evoked for women. The section defines stalking as to follow a woman and contact, or attempt to contact the woman to foster personal interaction repeatedly despite a clear indication of disinterest by the aggrieved woman; or monitor the use by a woman of the internet, email or any other form of electronic communication. There are exceptions to this section which include such act being in course of preventing or detecting a crime authorized by state or in compliance of certain law or was reasonable and justified.”*

“Section 370 has been substituted with new sections, 370¹⁰⁹ and 370A¹¹⁰ which deal with trafficking of person for exploitation. If a person (a) recruits, (b) transports, (c) harbors, (d) transfers, or (e) receives, a person, by using threats, or force, or coercion, or abduction, or fraud, or deception, or by abuse of power, or inducement for exploitation including prostitution, slavery, forced organ removal, etc. will be punished with imprisonment ranging from at least 7 years to imprisonment for the remainder of that person’s natural life depending on the number

¹⁰⁷ *Supra* note 97 s. 7

¹⁰⁸ *Id.*

¹⁰⁹ *Id.* s. 8

¹¹⁰ *Id.*

or category of persons trafficked. Employment of a trafficked person will attract penal provision as well.”

One of the major changes that have been included is pertaining to the offense of rape, while the Ordinance wanted to change the word rape to sexual assault, but the word rape has been kept in Section 375¹¹¹, and was extended to include acts in addition to vaginal penetration. The definition is broadly worded with acts like penetration of penis, or any object or any part of body to any extent, into the vagina, mouth, urethra or anus of another person or making another person do so, applies of mouth or touching private parts constitutes the offence of sexual assault. The section has also clarified that penetration means penetration to any extent, and lack of physical resistance is immaterial for constituting an offence. Except in certain aggravated situation the punishment will be imprisonment not less than seven years but which may extend to imprisonment for life, and shall also be liable to fine. In aggravated situations, punishment will be rigorous imprisonment for a term which shall not be less than ten years but which may extend to imprisonment for life, and shall also be liable to fine.

Section 376A has been added which states that if a person committing the offence of sexual assault, inflicts an injury which causes the death of the person or causes the person to be in a persistent vegetative state, shall be punished with rigorous imprisonment for a term which shall not be less than twenty years, but which may extend to imprisonment for life, which shall mean the remainder of that person's natural life, or with death.

In case of gang rape under Section 376D, persons involved regardless of their gender would be punished with rigorous imprisonment for a term which shall not be less than twenty years, but which may extend to life and shall pay compensation to the victim which shall be reasonable to meet the medical expenses and rehabilitation of the victim. The age of consent in India has been increased to 18 years, which means any sexual activity irrespective of presence of consent with a woman below the age of 18 will constitute statutory rape.

The amendment act also brought changes in the Indian Evidence Act and Code of Criminal Procedure. The process of recording the victim's statement is made easy and victim friendly. The most important changes brought by the Criminal Amendment act are that the court

¹¹¹ *Supra* note 97 s. 9

cannot cast doubt on the character of victim as it is made irrelevant in the offence of rape¹¹², and secondly the court from the first day presume no consent if it said by the victim in her statement to the court that she did not consent to act, where sexual intercourse is proved.¹¹³

The Dowry Prohibition Act, 1961 was also amended for this purpose. The changes have made the definition of dowry wider and cruelty by husband or relatives of the husband has become a crime, if the wife dies within seven years of marriage under suspicious circumstances, the husband and his relatives will have to prove that they had no hand in killing the bride if there is a history of torture and harassment of wife. But nothing much has improved by these legal amendments. All the crimes committed against women have maintained their upward trend. It has been found by various studies that most of the prosecution drops out at initial stage, either because of lethargy by police, faults of investigating agency and slow pace of judicial proceeding.

Suppression of Immoral Traffic in women and Girls Act 1956 was passed to prevent the evil of Immoral Trafficking. Section 366-A and 366-B were added to Indian Penal Code by the amendment in 2013 to make the procreation of minor girl a crime.

The Immoral Traffic (Prevention) Act 1986 was enacted with more stringent provisions to combat new forms of criminal trafficking and to protect innocent girls. Despite all these steps the flesh trade has assumed wide extraterritorial dimension. Girls are lured on promises of jobs but sold to brothels. What is more shocking is that they are often sold by their wars. The law is weak and in most of the cases, flesh trade and sale of minor girls goes on with the connivance of police. There are crimes that are committed within the four walls of the house, some are committed outside the house in lonely places and some at public places in spite of protective laws the index of these crimes is touching heights.

In *Deepak Gulathi v. State of Haryana*¹¹⁴, the Hon'ble Supreme Court on the consequences of rape on the women has held that Rape is the most morally and physically reprehensive crime in a society, as it is an assault on the body, mind and on privacy of the victim. While a murderer destroys the physical frame of the victim, a rapist degrades and defiles the soul

¹¹² The Indian Evidence Act, 1872, s. 53A

¹¹³ *Id.* s. 114A

¹¹⁴ *Deepak Gulathi v. State of Haryana* (2013) 7 SCC 675.

of the helpless female. Rape reduces a woman to an animal, as it shakes the very core of her life. By no means can a rape victim be called an accomplice. Rape leaves a permanent scar on the life of the victim, and therefore, a rape victim is placed on a higher pedestal than an injured witness. Rape is a crime against the entire society and violated the human rights of the victim. Being the most hated crime, rape tantamount to serious blow to the supreme Honour of the women, and affects both, her esteem and dignity. It causes physical and psychological harm to the victim, leaving upon her indelible marks.

5.4 Judicial Approach:

Laws have taken silent and slow steps in the direction of political participation of women preventing gender biases and removing lacunas in procedural laws and laws relating to evidence. The law cannot change a society overnight, but it can certainly ensure that the disadvantaged are not given a raw deal. The courts can certainly go beyond mere legality insulating women against injustice suffered due to biological and sociological factors.

But all law is not justice; nor is all justice law alone. At times there could be more justice without law and likewise there could be times when strict adherence to, or mindless application of laws, could lead to injustice. Justice is a combination of various factors: enactment of laws responsive to the changing needs of time, their effective enforcement, progressive and proactive interpretation and application so as to fill up any void that is left and not taken care of by statutory enactments. It is the law in action and not just the law which is important. If one were to ask to name a significant single factor which could make the delivery of justice, just and meaningful, the answer would be a sensitized judiciary, a judiciary which views the circumstances and situation in a holistic manner. Judges too have their own philosophy and their own convictions depending on the background wherefrom they come, but then, there is a collective qualitative philosophy of justice dispensation in which personal inhibitions and predilections have no place.

Judiciary in India has always played a laudable role in eradicating social evils, and to bring social justice to masses. The Supreme Court of India has devised various ways like epistolary jurisdiction, relaxing locus standi principle, allowing Public Interest Litigation (PIL) and has played pro-active role for bringing justice to every doorstep.

The Supreme Court in *Mahesh v. State of M.P.*¹¹⁵ has said “It will be a mockery of justice to permit the accused to escape the extreme penalty of law when faced with such evidence and such cruel acts. To give the lesser punishment for the accused would be to render the justice system of the country suspect. The common man will lose faith in courts. In such cases, he understands and appreciates the language of deterrence more than the reformatory terminology.”

The Supreme Court in *Dhananjay Chatterjee v. State of West Bengal*¹¹⁶ held that “In recent years, the rising crime rate-particularly violent crime against women has made the criminal sentencing by the courts a subject of concern. Today there are admitted disparities. Some criminals get very harsh sentences while many receive grossly different sentence for an essentially equivalent crime and a shockingly large number even go unpunished, thereby encouraging the criminal and in the ultimate making justice suffer by weakening the system’s credibility. Of course, it is not possible to lay down any cut and dry formula relating to imposition of sentence but the object of sentencing should be to see that the crime does not go unpunished and the victim of crime as also the society has the satisfaction that justice has been done to it. In imposing sentences, in the absence of specific legislation, Judges must consider variety of factors and after considering all those factors and taking an over-all view of the situation, impose sentence which they consider to be an appropriate one. Aggravating factors cannot be ignored and similarly mitigating circumstances have also to be taken into consideration. In our opinion, the measure of punishment in a given case must depend upon the atrocity of the crime; the conduct of the criminal and the defenseless and unprotected state of the victim. Imposition of appropriate punishment is the manner in which the courts respond to the society’s cry for justice against the criminals. Justice demands that courts should impose punishment fitting to the crime so that the courts reflect public abhorrence of the crime. The courts must not only keep in view the rights of the criminal but also the rights of the victim of crime and the society at large while considering imposition of appropriate punishment.”

Judiciary on Rape & Sexual Harassment:

The Apex Court of India has taken a stern view for crimes against women and specially rape. Time to time various directions has been issued by Court to protect women and penalize

¹¹⁵ *Mahesh v. State of M.P.* (1987) 2 SCR 710.

¹¹⁶ *Dhananjay Chatterjee v. State of West Bengal* (1994) 2 SCC 220.

the perpetrators of these horrible acts. The Apex Court called for a complete overhaul of the system for curbing the spurt in crime against women, including rape and sexual harassment, saying only deterrent punishment will be effective. In this chapter the researcher has cited out leading case laws which highlight the role of judiciary to curb the crime against woman and also issued number of guidelines to protect the victims.

In the *Chairman, Railway Board & Ors v. Mrs. Chandrima Das & Ors*¹¹⁷, supreme court observed that it is not a mere matter of violation of an ordinary right of a person but the violation of Fundamental Rights which is involved., as Smt. Hanuffa Khatoon was a victim of rape.

In *Bodhisatwa v. Ms. Subdhra Chakraborty*¹¹⁸, the Supreme Court has held rape as a crime which is offensive to the Fundamental Right of a person guaranteed under Article 21 of the Constitution. The Supreme Court further pointed out that Rape is a crime not only against the person of a women, it is a crime against the entire society. It destroys the entire psychology of women and pushes her into deep emotional crisis. Rape is therefore the most hated crime. It is a crime against basic human rights and is violative of the victims most cherished right to life which includes right to live with human dignity, contained in Article 21.

Bhanwari Devi Gang Rape Case:¹¹⁹ Bhanwari Devi is dalit social-worker from Bhatari, Rajasthan, who was allegedly gang raped in 1992 by higher-caste men infuriated by her efforts to put a stop to child marriage in their family. Her following treatment by the police, and court acquittal of the accused, attracted widespread national and international media attention, and became a landmark episode in India's women's rights movement. The Gender bias at that point of time prevalent in Indian Judiciary at that point of time that is shown with the verdict in Bhanwari Devi case. Judge Jagpal Singh's in his 26 page verdict has stated that it isn't possible in Indian culture that a man who has taken a vow to protect his wife, in front of the holy fire, just stands and watches his wife being raped, when only two men almost twice his age are holding him. The Verdict also states that the accused, there were three brothers and an uncle, and it's highly improbable that an uncle and his nephews would commit rape together. The judge also observes that gangs in rural areas are not usually multicast and, therefore, the accusation that

¹¹⁷ *Chairman, Railway Board & Ors v. Mrs. Chandrima Das & Ors* (2000) 2 SCC 465.

¹¹⁸ *Bodhisatwa v. Ms. Subdhra Chakraborty* (1996) 1 SCC 490.

¹¹⁹ *Vishakha and others v State of Rajasthan*, AIR 1997 SC 3011.

they acted together is highly impossible. Moreover, he endorses the defence counsel's view that Indian rural society couldn't have sunk so low that a villager would lose all sense of age and caste and pounce upon a woman like a wolf. The Statement like these by the Judge has prompted women's organizations to brand it the personification of gender bias in the judiciary. This led a women's rights group called Vishaka that filed PIL in the Apex Court of India. The PIL has been filed for the enforcement of the fundamental rights of working women under Articles 14, 19 and 21 of the Constitution of India in view of the existing environment in which the violation of these rights is not unusual. With the increasing understanding and importance on gender justice, there is increase in the effort to guard such infringement; and there is lack of sympathy towards incidents of sexual harassment is also increasing. The current appeal has been brought as a class action by certain social activists and NGOs with the aim of focusing attention towards this communal deviation, and assisting in finding appropriate methods for recognition of the true concept of gender parity; and to stop sexual pestering of working women in all work places through judicial practice, to fill the void in existing legislation.

The Supreme Court also stated that "each such incident results in violation of the fundamental rights of Gender Equality and the Right to Life and Liberty. It is a clear violation of the rights under Arts. 14, 15 and 21 of the Constitution. One of the logical consequences of such an incident is also the violation of the victim's fundamental right under Art. 19 (1) (g) to practice any profession or to carry out any occupation, trade or business. Such violations, therefore, attract the remedy under Art. 32 for the enforcement of these fundamental rights of women. This class action under Art. 32 of the Constitution are for this reason. A writ of mandamus in such a situation, if it is to be effective, needs to be accompanied by directions for prevention; as the violation of fundamental rights of this kind is a recurring phenomenon. The fundamental right to carry on any occupation, trade or profession depends on the availability of a safe working environment. Right to life means life with dignity. The primary responsibility for ensuring such safety and dignity through suitable legislation, and the creation of a mechanism for its enforcement, is of the legislature and the executive. When, however, instances of sexual harassment resulting in violation of fundamental rights of women workers under Arts. 14, 19 and 21 are brought before us for redress under Art 32; an effective redressal requires that some guidelines should be laid down for the protection of these rights to fill the legislative vacuum."

In the year 1997, the Supreme Court passed a landmark judgment and set down guiding principle to be followed by establishments in dealing with grievances about sexual pestering at workplace. The Supreme Court also stated that these rule were to be implemented until legislation is passed to deal with the issue.

After that the Vishaka Case, the Supreme Court in Medha Kotwal case¹²⁰ , the Hon'ble Supreme Court directed that the Complaints Committees shall be deemed to be the Inquiry Authority for the purpose of Central Civil Services (Conduct) Rules, 1964 and that the report of the Complaints Committees will be deemed to be the Inquiry Report under the Rules.

The Supreme Court also in Seema Lepcha v. State of Sikkim & Ors¹²¹ upholding the judgment in Vishaka Case and Medha Kotwal Case given following direction/guidelines regarding implementation of the guidelines by the state government:

- “The State Government shall give comprehensive publicity to the notifications and orders issued by it in compliance of the guidelines framed by this Court in Vishaka’s case and the directions given in Medha Kotwal case by getting the same published in the newspapers having maximum circulation in the State after every two months;
- Wide publicity be given every month on Doordarshan Station, Sikkim about various steps taken by the State Government for implementation 10 of the guidelines framed in Vishaka’s case and the directions given in Medha Kotwal case;
- Social Welfare Department and the Legal Service Authority of the State of Sikkim shall also give wide publicity to the notifications and orders issued by the State Government not only for the Government departments of the State and its agencies / instrumentalities but also for the private companies.”

Till 2013 these guidelines protect the rights of individuals against sexual harassment at the workplace when the government of India passed The Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013 which seeks to protect women from sexual harassment at their workplace. The basic objective of the act to provide protection

¹²⁰ Medha Kotwal Lele v. Union of India (2013) 1 SCC 311.

¹²¹ Seema Lepcha v. State of Sikkim & Ors (2013) 11 SCC 647.

against sexual pestering of women at workplace and for the prevention and redressal of complaints of sexual harassment and for matters associated with or related to.

Responsibility of the Courts in Handling Cases related to the Crimes against women:

In *Shyam Narain v. State, NCT of Delhi*¹²², the Supreme Court has openly talked about the judicial behaviour regarding crime against woman and said almost for the last three decades, the Supreme Court has been expressing its agony and distress pertaining to the increased rate of crimes against women. The eight year old girl (brutally raped by appellant), who was supposed to spend time in cheerfulness, was dealt with animal passion and her dignity and purity of physical frame was shattered. The plight of the child and the shock suffered by her can be well visualized. The torment on the child has the potentiality to corrode the poise and equanimity of any civilized society. The age-old wise saying that child is a gift of the providence enters into the realm of absurdity. The young girl, with efflux of time, would grow with a traumatic experience, an unforgettable shame. She shall always be haunted by the memory replete with heavy crush of disaster constantly echoing the chill air of the past forcing her to a state of nightmarish melancholia. She may not be able to assert the honor of a woman for no fault of hers. When she suffers, the collective at large also suffers.

The Supreme Court in this case further explained Respect for reputation of women in society shows the basic civility of a civilized society. No member of society can afford to conceive the idea that he can create a hollow in the honour of women. Such thinking is not only lamentable but also deplorable. It would not be an examination to say that the thought of sullyng the physical frame of a woman is the demolition of the excepted civilized norm.

The Supreme Court also in *Gurnaib Singh v. State of Punjab*¹²³ held that *“It is a matter of great shame and grave concern that brides are burnt or otherwise their life sparks are extinguished by torture, both physical and mental, because of demand of dowry and insatiably greed and sometimes, sans demand of dowry, because of the cruelty and harassment made it out to the nascent brides treating them with total insensitivity destroying their desire to live and forcing them to commit suicide; a brutal self-humiliation of life.”*

¹²² *Shyam Narain v. State, NCT of Delhi* (2013) 7 SCC 77.

¹²³ *Gurnaib Singh v. State of Punjab* (2013) 7 SCC 108.

The Supreme Court in dealing with above case also explained the position of Indian families “Respect of a bride in her matrimonial home glorified the solemnity and sanctity of marriage, reflects the sensitivity of a civilized society and, eventually atomized her aspiration, dreamt of in nuptial bliss. But, the manner in which sometimes the brides are treated in many a home by the husband, in-laws and relatives creates a feeling of emotional numbness in the society. Daughter-in-law is to be treated as a member of the family with warm and effect and not as a stranger with despicable and ignoble indifference. She should not be treated as a housemaid. No impression should be given that she can be thrown out from her matrimonial home at any time.”

It gives an idea about the sensitiveness and responsiveness of higher Courts, the Supreme Court and the High Courts, regarding the crimes against women after the Nirbhaya incident. It is most likely that the overall increase in reporting is a result of enhanced awareness amongst women and their family/support systems combined with directions of Hon’ble Supreme Court in *Lalita Kumar v. Government of Uttar Pradesh*¹²⁴ regarding mandatory registration of FIR in cognizable cases and the introduction of Section 166A of Cr.P.C which makes its breach, punishable. Increased media rendezvous on the issue of crime against women has also played its part in mainstreaming and creating better understanding about the legal remedies available. While it is hard to depict a direct association between better public awareness and increased coverage of Crime against Woman, it is definitely likely to smooth the progress of women’s access to justice by making domestic & other social support structures more supportive. The Supreme Court issued the following Guidelines regarding the registration of FIR.

- “Registration of FIR is mandatory under Section 154 of the Code, if the information discloses commission of a cognizable offence and no preliminary inquiry is permissible in such a situation;
- If the information received does not disclose a cognizable offence but indicates the necessity for an inquiry, a preliminary inquiry may be conducted only to ascertain whether cognizable offence is disclosed or not;
- If the inquiry discloses the commission of a cognizable offence, the FIR must be registered. In cases where preliminary inquiry ends in closing the complaint, a copy of

¹²⁴ *Lalita Kumar v. Government of Uttar Pradesh* (2014) 2 SCC 1.

the entry of such closure must be supplied to the first informant forthwith and not later than one week. It must disclose reasons in brief for closing the complaint and not proceeding further.

- The police officer cannot avoid his duty of registering offence if cognizable offence is disclosed. Action must be taken against erring officers who do not register the FIR if information received by him discloses a cognizable offence;
- The scope of preliminary inquiry is not to verify the veracity or otherwise of the information received but only to ascertain whether the information reveals any cognizable offence;
- As to what type and in which cases preliminary inquiry is to be conducted will depend on the facts and circumstances of each case;
- While ensuring and protecting the rights of the accused and the complainant, a preliminary inquiry should be made time bound and in any case it should not exceed 7 days. The fact of such delay and the causes of it must be reflected in the General Diary entry;
- Since the General Diary/Station Diary/Daily Diary is the record of all information received in a police station, we direct that all information relating to cognizable offences, whether resulting in registration of FIR or leading to an inquiry, must be mandatorily and meticulously reflected in the said Diary and the decision to conduct a preliminary inquiry must also be reflected, as mentioned above.”

Sensitive Approach in cases of Sexual Assault of Children:

In *State of Rajasthan v. Om Prakash*¹²⁵ the Supreme Court herein observed that It is necessary for the courts to have a sensitive approach when dealing with cases of child rape. The effect of such a crime on the mind of the child is likely to be lifelong. A special safeguard has been provided for children in the Constitution of India in Article 39 which, inter alia, stipulates that the State shall, in particular, direct its policy towards securing that the tender age of the children is not abused and the children are given opportunities and facilities to develop in a healthy manner and in conditions of freedom and dignity and that the childhood and youth are protected against exploitation and against moral and material abandonment.

¹²⁵ *State of Rajasthan v. Om Prakash* (2002) 5 SCC 745.

In the present case, the victim at the time of occurrence of rape was a child aged eight years. The accused was youth aged 18 years. The house of the accused was quite close to that of the prosecutrix. The FIR was registered in this case on the next day of the occurrence of the incident. Herein the Court reiterated the proposition while referring to the cases of *State of Punjab v. Gurmit Singh*¹²⁶, and *State of Maharashtra v. Chandraprakash Kewal Chand Jain*¹²⁷, that the conviction for offence under Section 376 IPC can be based on the sole testimony of a rape victim. In the abovementioned cases the Supreme Court held that, it must not be overlooked that a women or a girl subjected to sexual assault is not an accomplice to the crime but is a victim of another person's lust and it is improper and undesirable to test her evidence with a certain amount of suspicion, treating her as if she were an accomplice.

Justice A.S. Anand speaking for the court was referred stating that the inherent bashfulness of the females and the tendency to conceal outrage of sexual aggression are factors which the courts should not overlook.

The Court disapproved of the approach taken by the High Court and held that the High Court has clearly committed a serious illegality in assuming that in natural course of events if rape had been committed, the young child girl and her mother would have shouted so as to collect others and they would have visited her house. The prosecutrix was unconscious. There was no question of prosecutrix shouting as assumed by the High Court. Too much was made by the High Court on account of non-examination of persons other than the family members. The cases involving sexual molestation and assault require a different approach a sensitive approach and not an approach which a court may adopt in dealing with a normal offence under penal laws.

The Court negated the contention that the revenge on account of alleged dispute regarding exchange of land would be taken by the father of the prosecutrix by foisting on the accused a false case of rape involving his young daughter particularly in the setting of a village environment. The conviction could not be set aside for the non-examination of independent witness. Thus his conviction was reinstated for offence under Section 376, Indian Penal Code

¹²⁶ *State of Punjab v. Gurmit Singh* (1996) 2 SCC 384.

¹²⁷ *State of Maharashtra v. Chandraprakash Kewal Chand Jain*, (1990) 1 SCC 550.

and rigorous imprisonment for seven years was imposed with fine of Rs.1,000/- and in default of payment of fine to further undergo six months rigorous imprisonment.

Court cannot disgrace the character of a victim:

In *State of Punjab v. Gurmit Singh & Ors*¹²⁸ the Supreme Court in this landmark judgment come out with numbers of observation stated below:

Crime against women in general and rape in particular is on the increase. It is an irony that while we are celebrating women's rights in all spheres, we show little or no concern for her honour. It is a sad reflection on the attitude of indifference of the society towards the violation of human dignity of the victims of sex crimes. We must remember that a rapist not only violates the victim's privacy and personal integrity, but inevitably causes serious psychological as well as physical harm in the process. Rape is not merely a physical assault - it is often destructive of the whole personality of the victim. A murderer destroys the physical body of his victim; a rapist degrades the very soul of the helpless female. The Courts, therefore, shoulder a great responsibility while trying an accused on charges of rape. They must deal with such cases with utmost sensitivity. The Courts should examine the broader probabilities of a case and not get swayed by minor contradictions or insignificant discrepancies in the statement of the prosecutrix, which are not of a fatal nature, to throw out an otherwise reliable prosecution case. If evidence of the prosecutrix inspires confidence, it must be relied upon without seeking corroboration of her statement in material particulars. If for some reason the Court finds it difficult to place implicit reliance on her testimony, it may look for evidence which may lend assurance to her testimony, short of corroboration required in the case of an accomplice. The testimony of the prosecutrix must be appreciated in the background of the entire case and the trial court must be alive to its responsibility and be sensitive while dealing with cases involving sexual molestations.

The court, therefore, should not sit as a silent spectator while the victim of crime is being cross-examined by the defence. It must effectively control the recording of evidence in the court. While every latitude should be given to the accused to test the veracity of the prosecutrix and the credibility of her version through cross-examination, the court must also ensure that

¹²⁸ *State of Punjab v. Gurmit Singh & Ors*, A.I.R. 1996 S.C. 1393.

cross-examination is not made a means of harassment or causing humiliation to the victim of crime.

The Supreme Court while coming heavily on trial court and setting aside the judgment said that the trial court not only erroneously disbelieved the prosecutrix, but quite uncharitably and unjustifiably even characterised her as a girl of loose morals or such type of a girl.

What has surprised our judicial beliefs all the more is the conclusion drawn by the court, based on no proof and not even on a denied submission, to the effect:

The more probability is that (prosecutrix) was a girl of loose character. She wanted to dupe her parents that she resided for one night at the house of her maternal uncle, but for the reasons best known to her she does not do so and she preferred to give company to some persons.

The Apex Court strongly criticized the approach of the trial court and stated that the observations lack sobriety expected of a Judge. Such like stigmas have the potential of not only discouraging an even otherwise redutant victim of sexual assault to bring forth complaint for trial of criminals, thereby making the society to suffer by letting the criminal escape even a trial. The courts are expected to use self- restraint while recording such findings which have larger repercussions so far as the future of the victim of the sex crime is concerned and even wider implications on the society as a whole-where the victim of crime is discouraged. The criminal encouraged and in turn crime gets rewarded. Even in cases, unlike the present case, where there is some acceptable material on the record to show that the victim was habituated to sexual intercourse, no such inference like the victim being a girl of loose moral character is permissible to be drawn from that circumstance alone. Even if the prosecutrix, in a given case, has been promiscuous in her sexual behaviour earlier, she has a right to refuse to submit herself to sexual intercourse to anyone and everyone because she is not a vulnerable object or prey for being sexually assaulted by anyone had everyone. No stigma, like the one as cast in the present case should be cast against such a witness by the Courts, for after all it is the accused and not the victim of sex crime who is on trial in the Court.

The courts are obliged to act in furtherance of the intention expressed by the legislature and not to ignore its mandate and must invariably take recourse to the provisions of Section

327(2) and (3) Cr.P.C and hold the trial of rape cases in camera. It would enable the victim of crime to be a little comfortable and answer the questions with greater ease in not too familiar surroundings. Trial in camera would not only be in keeping with the self-respect of the victim of crime and in tune with the legislative intent but is also likely to improve the quality of the evidence of a prosecutrix because she would not be so hesitant or bashful to depose frankly as she may be in an open court, under the gaze of public. The improved quality of her evidence would assist the courts in arriving at the truth and sifting truth from falsehood.

Wherever possible, it may also be worth considering whether it would not be more desirable that the cases of sexual assaults on the females are tried by lady Judges, wherever available, so that the prosecutrix can make her statement with greater ease and assist the courts to properly discharge their duties, without allowing the truth to be sacrificed at the altar of rigid technicalities while appreciating evidence in such cases. The courts should, as far as possible, avoid disclosing the name of the prosecutrix in their orders to save further embarrassment to the victim of sex crime. The anonymity of the victim of the crime must be maintained as far as possible throughout. In the present case, the trial court has repeatedly used the name of the victim in its order under appeal, when it could have just referred to her as the prosecutrix.

Rehabilitation of Sex Workers:

Retired Justice Markandey Katju and Gyan Sudha Misra in the case of *Budhadev Karmaskar v. State Of West Bengal*¹²⁹ observed that the Central and the State Governments through Social Welfare Boards should prepare schemes for rehabilitation all over the country for physically and sexually abused women commonly known as prostitutes as we are of the view that the prostitutes also have a right to live with dignity under Article 21 of the Constitution of India since they are also human beings and their problems also need to be addressed.

As affirmed a woman is compelled to indulge in prostitution not for pleasure but because of abject poverty. If such a woman is granted opportunity to avail some technical or vocational training, she would be able to earn her livelihood by such vocational training and skill instead of by selling her body.

¹²⁹ *Budhadev Karmaskar v. State Of West Bengal* (2011) 10 SCR 577.

Hence, we direct the Central and the State Governments to prepare schemes for giving technical/vocational training to sex workers and sexually abused women in all cities in India. The schemes should mention in detail who will give the technical/vocational training and in what manner they can be rehabilitated and settled by offering them employment. For instance, if a technical training is for some craft like sewing garments, etc. then some arrangements should also be made for providing a market for such garments, otherwise they will remain unsold and unused, and consequently the women will not be able to feed her.

The petitioner in *Gaurav Jain v. Union of India*¹³⁰ prayed for establishing separate educational institutions for the children of the fallen women. The SC observed that segregating children of prostitutes by locating separate schools and providing separate hostels would not be in the interest of the children and the society at large. The Supreme Court did not accept the plea for separate hostels for children of prostitutes, but it felt that accommodation in hostels and other reformatory homes should be adequately available to help segregation of these children from their mothers living in prostitute homes as soon as they are identified.

In its judgment, the Supreme Court quoted the Fundamental Rights of women and children from the Constitution of India and relevant international instruments. The court deliberated on the reasons for prostitution and the continuation of the victims in profession and recognized that the victims are the poor, illiterate and ignorant sections of the society who are the target group in the flesh trade; rich communities exploit them and harvest at their misery and humiliation in an organized way, in particular, with police nexus. The court held that women found in the flesh trade, should be viewed more as victims of adverse socio-economic circumstances rather than as offenders in our society. Equally, the right of the child is the concern of the society so that fallen women surpass trafficking of her person from exploitation; contribute to bring up her children; live a life with dignity; and not to continue in the foul social environment. Equally, the children have the right to equality of opportunity, dignity and care, protection and rehabilitation by the society with both hands open to bring them into the mainstream of social life without prestigma affixed on them for no fault of her/his.

¹³⁰ *Gaurav Jain v. Union of India*, A.I.R. 1990 S.C. 292.

The SC stated that three Cs, viz., Counselling, Cajoling and Coercion were necessary to effectively enforce the provisions of various statutes. The role of NGOs in rehabilitating and educating the children of the fallen women was emphasized. Detailed directions were given for rescue, rehabilitation of prostitutes and children of prostitutes. The SC held that society was responsible for a woman becoming a victim of circumstances therefore; society should make reparation to prevent trafficking in women, rescue them from red light areas and other areas in which the women were driven or trapped in prostitution. Their rehabilitation by socio-economic empowerment and justice is the constitutional duty of the State. Their economic empowerment and social justice with dignity of person are the fundamental rights and the Court and the Government should positively endeavour to ensure them.

The Hon'ble Supreme Court in Vishal Jeet v. Union of India¹³¹ explained the pathetic situation of the victims:

No denying the fact that prostitution always remains as a running sore in the body of civilization and destroys all moral values. The causes and evil effects of prostitution maligning the society are so notorious and frightful that none can gainsay it. This malignity is daily and hourly threatening the community at large slowly but steadily making its way onwards leaving a track marked with broken hopes. Therefore, the necessity for appropriate and drastic action to eradicate this evil has become apparent but its successful consummation ultimately rests with the public at large.

It is highly deplorable and heart-rending to note that many poverty stricken children and girls in the prime of youth are taken to flesh market and forcibly pushed into the flesh trade which is being carried on in utter violation of all canons of morality, decency and dignity of humankind. There cannot be two opinions, indeed there is none, that this obnoxious and abominable crime committed with all kinds of unthinkable vulgarity should be eradicated at all levels by drastic steps.

The Hon'ble Supreme Court has directed certain guidelines for eradication of the problem:

¹³¹ Vishal Jeet v. Union of India A.I.R. 1990 S.C. 1412.

This devastating malady can be suppressed and eradicated only if the law enforcing authorities in that regard take very severe and speedy legal action against all the erring persons such as pimps, brokers and brothel keepers. The Courts in such cases have to always take a serious view of this matter and inflict consign punishment on proof of such offences. Apart from legal action, both the Central and the State Government who have got an obligation to safeguard the interest and welfare of the children and girls of this country have to evaluate various measures and implement them in the right direction.

Judiciary & Khap Panchayat (Honor Killing):

The words honour killings and honour crimes are being used loosely as convenient expressions to describe the incidents of brutality and pestering caused to the young couple planning to marry or having married against the desires of the society or family members. They are used more as catch phrases and not as appropriate and accurate expressions. The so-called honour killings or honour crimes are not peculiar to our country. It is an evil which haunts many other societies also. The belief that the victim has brought dishonor upon the family or the community is the root cause of such violent crimes. Such violent crimes are directed especially against women. Men also become targets of attack by members of family of a woman with whom they are perceived to have an inappropriate relationship. Changing cultural and economic status of women and the women going against their male dominated culture has been one of the causes of honour crimes. In some western cultures, honour killings often arise from women seeking greater independence and choosing their own way of life. In some cultures, honour killings are considered less serious than other murders because they arise from long standing cultural traditions and are thus deemed appropriate or justifiable. An adulterous behaviour of woman or pre-marital relationship or assertion of right to marry according to their choice, are widely known causes for honour killings in most of the countries.

The rising incidence of commission of murders of persons marrying outside their caste or religion and other serious offences perpetrated or hostility generated against them and also causing harm to their close relatives or a section of the community on considerations of caste and gotra are matters of grave concern. Those who may be directly involved in the actual commission of acts of violence or murder are either part of a community or section of the people and may also include members of the family concerned in the case of objected marriages. Very

often such incidents and offences are not even taken cognizance at the threshold. The domineering position and strength wielded by caste combinations and assemblies, silence or stifle the investigating and prosecuting agencies.

The pernicious practice of Khap Panchayat and the like taking law into their own hands and pronouncing on the invalidity and impropriety of Sagotra and inter-caste marriages and handing over punishment to the couple and pressurizing the family members to execute their verdict by any means amounts to flagrant violation of rule of law and invasion of personal liberty of the persons affected.

The Apex Court in *Lata Singh v. State of U.P.*¹³² observed and directed the caste system is a curse on the nation and the sooner it is destroyed the better. In fact, it is dividing the nation at a time when we have to be united to face the challenges before the nation unitedly. Hence, inter-caste marriages are in fact in the national interest as they will result in destroying the caste system. However, disturbing news are coming from several parts of the country that young men and women who undergo inter-caste marriage, are threatened with violence, or violence is actually committed on them. In our opinion, such acts of violence or threats or harassment are wholly illegal and those who commit them must be severely punished. This is a free and democratic country, and once a person becomes a major he or she can marry whosoever he/she likes. If the parents of the boy or girl do not approve of such inter-caste or inter-religious marriage the maximum they can do is that they can cut off social relations with the son or the daughter, but they cannot give threats or commit or instigate acts of violence and cannot harass the person who undergoes such inter-caste or inter-religious marriage. We therefore, direct that the administration/police authorities throughout the country will see to it that if any boy or girl who is a major undergoes inter-caste or inter-religious marriage with a woman or man who is a major, the couple are not harassed by any one nor subjected to threats or acts of violence, and anyone who gives such threats or harasses or commits acts of violence either himself or at his instigation, is taken to task by instituting criminal proceedings by the police against such persons and further stern action is taken against such persons as provided by law. We sometimes hear of honour killings of such persons who undergo inter-caste or inter-religious marriage of their own free will. There is nothing honorable in such killings, and in fact they are nothing but barbaric

¹³² *Lata Singh v. State of U.P.* (2006) 5 SCC 475.

and shameful acts of murder committed by brutal, feudal minded persons who deserve harsh punishment. Only in this way can we stamp out such acts of barbarism.

In *Pradeep Kumar Singh v. State of Haryana*¹³³ the High Court of Punjab and Haryana has laid down the guidelines to pertaining to the handling of the complaints against the runaway couple and their parents. The direction issued in the judgment is following:

- “Whenever any intimation is received by the SSP/SP of concerned District regarding the marriage of a young couple with a threat and an apprehension of infringement of the right of life and liberty by the police at the instance of the family members of one of the spouses, the SSP/SP concerned will consider the representation and will himself/herself look into the matter and issue necessary directions to maintain a record of the said intimation under Chapter 21 of the Punjab Police Rules;
- On receipt of above said intimation of marriage by any police officer, necessary directions will be issued to the concerned Police Station to take necessary steps in accordance with law to enquire into the matter by contracting the parents of both boy and girl. The matter regarding age, consent of the girl and grievance of her family will be determined. In the eventuality of any complaint of kidnapping or abduction having been received from any of the family members of the girl generally the boy (husband) will not be arrested unless and until the prejudicial statement is given by the girl (wife). Arrest should generally be deferred or avoided on the immediate receipt of a complaint by the parents or family members of the girl taking into consideration the law laid down by Hon’ble Supreme Court in *Joginder Kumar’s* case;
- If the girl is major (above 18 years), she should not forcibly be taken away by police to be handed over to her parents against her consent. Criminal force against the boy should also be avoided;
- So far as the threat to the young couple of the criminal force and assault at the hands of the private persons is concerned, it would always be open to the police to initiate action if any substantive offence is found to have been committed against the couple;

¹³³ *Pradeep Kumar Singh v. State of Haryana* (2008) 3 RCR 376.

- In case of any threat to the breach of peace at the hands of the family members of the couple it will always be open to the State authorities to take up the security proceedings in accordance with law;
- It will not be open to the runaway couple to take law in their hands pursuant to the indulgence shown by the police on the basis of their representation sent to the SSP/SP of the concerned District;
- If despite the intimation having been sent to the SSP/SP there is an apprehension or threat of violation of right of personal life and liberty or free movement, the remedy of approaching the High court should be the last resort;
- In case there is an authority constituted for issuance of marriage certificate as per the law in the concerned districts, the couple of so called run away marriage should get the marriage registered in compliance with the directions of the Supreme Court and a copy of the same should also be forwarded to the police along with the representations or anytime subsequent thereto.”

In *Arumugam Servai v. State of Tamil Nadu*¹³⁴, The Supreme Court strongly condemn the practice of khap panchayats and stated that in recent years Khap Panchayat (known as katta panchayats in Tamil Nadu) which often decree or encourage honour killings or other atrocities in an institutionalized way on boys and girls of different castes and religion, who wish to get married or have been married, or interfere with the personal lives of people. We are of the opinion that this is wholly illegal and has to be ruthlessly stamped out.

Hence, we direct the administrative and police officials to take strong measures to prevent such atrocious acts. If any such incidents happen, apart from instituting criminal proceedings against those responsible for such atrocities, the State Government is directed to immediately suspend the District Magistrate/Collector and SSP/SPs of the district as well as other officials concerned and charge sheet them and proceed against them departmentally if they do not (1) prevent the incident if it has not already occurred but they have knowledge of it in advance, or (2) if it has occurred, they do not promptly apprehend the culprits and others involved and institute criminal proceedings against them, as in our opinion they will be deemed to be directly or indirectly accountable in this connection.

¹³⁴ *Arumugam Servai v. State of Tamil Nadu* (2011) 6 SCC 405.

Retired Justice Markandey Katju and Justice Gyan Sudha Mishra have state that honour killings have become common place in many parts of the country, particularly in Haryana, western U.P., and Rajasthan. Often young couples who fall in love have to seek shelter in the police lines or protection homes, to avoid the wrath of kangaroo courts. In our opinion honour killings, for whatever reason, come within the category of rarest of rare cases deserving death punishment. It is time to stamp out these barbaric, feudal practices which are a slur on our nation. This is necessary as a deterrent for such outrageous, uncivilized behaviour. All persons who are planning to perpetrate honour killings should know that the gallows await them¹³⁵.

Legal Aid is a Constitutional Right:

By the 42nd Amendment to the Constitution of India, effected in 1977, Article 39-A was inserted. This Article provide for free legal assistance by suitable legislation or system or in any other way, to ensure that vision for securing justice are not deprived of any inhabitant on the grounds of economic and others. Article 39-A of the Constitution reads as follows the State shall secure that the operation of the legal system promotes justice, on a basis of equal opportunity, and shall, in particular, provide free legal aid, by suitable legislation or schemes or in any other way, to ensure that opportunities for securing justice are not denied to any citizen by reason of economic or other disabilities.¹³⁶

In *Hussainara Khatoon v. Home Secretary, State of Bihar*¹³⁷, The Supreme Court has held that free legal service is an inalienable element of “reasonable, fair and just procedure for a person accused of an offence and it must be held implicit in the guarantee of Article 21. It was noted that this is a constitutional right of every accused person who is unable to engage a lawyer and secure free legal services on account of reasons such as poverty, indigence or incommunicator situation. It was held that the State is under a mandate to provide a lawyer to an accused person if the circumstances of the case and the needs of justice so require, subject of course to the accused person not objecting to the providing of a lawyer.

¹³⁵ *Bhagwan das v. State (NCT) of Delhi* (2011) 6 SCC 396.

¹³⁶ INDIAN CONST. art. 39A.

¹³⁷ *Hussainara Khatoon v. Home Secretary, State of Bihar* (1980) 1 SCC 98.

In *Khatri v. State of Bihar*¹³⁸, The Supreme Court Expressing displeasure over disregard of the decision of the Supreme Court by the State of Bihar held that: The right to free legal services is clearly an essential ingredient of reasonable, fair and just procedure for a person accused of an offence and it is implicit in the guarantee of Article 21 and the State is under a constitutional mandate to provide a lawyer to an accused person if the circumstances of the case and the needs of justice so require, provided of course the accused person does not object to the provision of such lawyer. The State should provide free legal aid to an accused person who is unable to secure legal services on account of indigence and whatever is necessary for this purpose has to be done by the State. It cannot avoid its constitutional obligation to provide free legal services to a poor accused by pleading financial or administrative liability. The State is under a constitutional obligation to provide free legal services not only at the stage of trial but also at the stage when the accused is first produced before the magistrate as also when he is remanded from time to time.

But even this right to free legal services would be illusory for an indigent accused unless the magistrate or the Sessions Judge before whom he is produced informs him of such right. It would make a mockery of legal aid if it were to be left to a poor ignorant and illiterate accused to ask for free legal services. Legal aid would become merely a paper promise and it would fail of its purpose. The magistrate or the session's judge before whom the accused appears must be held to be under an obligation to inform the accused that if he is unable to engage the services of a lawyer on account of poverty or indigence, he is entitled to obtain free legal services at the cost of the State. Unless he is not willing to take advantage, every other State in the country should make provision for grant of free legal services to an accused that is unable to engage a lawyer on account of reasons such as poverty, indigence or in communicate situation. The only qualification would be that the offence charged against the accused is such that on conviction it would result in a sentence of imprisonment and is of such a nature that the circumstances of the case and the needs of social justice require that he should be given free legal representation. There may be cases involving offences such as economic offences or offences against law prohibiting prostitution or child abuse and the like, where social justice may require that free legal services need not be provided by the State.

¹³⁸ *Khatri v. State of Bihar* (1981) 1 SCC 627.

The State and its police authorities should see to it that the constitutional and legal requirement to produce an arrested person before a judicial magistrate within 24 hours of the arrest is scrupulously observed.

The provision inhibiting detention without remand is a very healthy provision which enables the magistrates to keep check over the police investigation and it is necessary that the magistrates should try to enforce this requirement and where it is found to be disobeyed come down heavily upon the police.

In *Suk Das v. Union Territory of Arunachal Pradesh*¹³⁹, The Supreme Court had reiterated that the requirement of providing free and adequate legal representation to an indigent person and a person accused of an offence. In that case, it was reiterated that an accused need not ask for legal assistance – the Court dealing with the case is obliged to inform him or her of the entitlement to free legal aid. This Court further observed that it was now settled law that free legal assistance at State cost is a fundamental right of a person accused of an offence which may involve jeopardy to his life or personal liberty and this fundamental right is implicit in the requirement of reasonable, fair and just procedure prescribed by Article 21 of Constitution of India.

Direction to Government:

In *CEHAT & Ors v. Union of India*¹⁴⁰, the Supreme Court admitting the lapse in implementation of laws banning sex selection / sex determination directed the central Government has ordered that It is unfortunate that for one reason or the other, the practice of female infanticide still prevails despite the fact that gentle touch of a daughter and her voice has soothing effect on the parents. One of the reasons may be the marriage problems faced by the parents coupled with the dowry demand by the so-called educated and/or rich persons who are well placed in the society. The traditional system of female infanticide whereby female baby was done away with after birth by poisoning or letting her choke on husk continues in a different form by taking advantage of advance medical techniques. Unfortunately, developed medical science is misused to get rid of a girl child before birth. Knowing full well that it is immoral and

¹³⁹ *Suk Das v. Union Territory of Arunachal Pradesh* (1986) 2 SCC 401.

¹⁴⁰ *CEHAT & Ors v. Union of India* (2001) 5 SCC 577.

unethical as well as it may amount to an offence; foetus of a girl child is aborted by qualified and unqualified doctors or compounders. This has affected overall sex ratio in various States where female infanticide is prevailing without any hindrance.

Court has to analyse the connection between demand of dowry/Cruelty and Death:

In *Bansi Lal v. State of Haryana*¹⁴¹ the Supreme Court observed that in each case, the court has to analyse the facts and circumstances leading to the death of the victim and decide if there is any proximate connection between the demand of dowry and act of cruelty or harassment and the death. That in Section 113B of the Indian Evidence Act, 1872 the legislature in its wisdom has used the word shall thus, making a mandatory application on the part of the court to presume that death had been committed by the person who had subjected her to cruelty or harassment in connection with or demand of dowry. It is unlike the provisions of Section 113A of the Evidence Act where discretion has been conferred upon the court wherein it had been provided that court may presume to abatement of suicide by a married woman. Therefore, in view of the above, onus lies on the accused to rebut the presumption and in case of Section 113B relating to Section 304 of IPC; the onus to prove shifts exclusively and heavily on the accused. Further, the SC stated that, in each case, the court has to analyse the facts and circumstances leading to the death of the victim and decide if there is any proximate connection between the demand of dowry and act of cruelty or harassment and the death.

In *Sunil Bajaj v. State of M.P.*¹⁴², the Apex Court held that we have given our attention and consideration to the submissions made by the learned counsel for the parties. Normally this Court will be slow and reluctant, as it ought to be, to upset the order of conviction of the trial court as confirmed by the High Court appreciating the evidence placed on record. But in cases where both the courts concurrently recorded a finding that the accused was guilty of an offence in the absence of evidence satisfying the necessary ingredients of an offence, in other words, when no offence was made out, it becomes necessary to disturb such an order of conviction and sentence to meet the demand of justice. In order to convict an accused for an offence under Section 304-B IPC, the following essentials must be satisfied: (1) the death of a woman must have been caused by burns or bodily injury or otherwise than under normal circumstances; (2)

¹⁴¹ *Bansi Lal v. State of Haryana*, A.I.R. 2011 S.C. 691.

¹⁴² *Sunil Bajaj v. State of M.P.* (2001) 9 SCC 417.

such death must have occurred within 7 years of her marriage; (3) soon before her death, the woman must have been subjected to cruelty or harassment by her husband or by relatives of her husband; (4) such cruelty or harassment must be for or in connection with demand of dowry.

Further stated that “It is only when the aforementioned ingredients are established by acceptable evidence such death shall be called dowry death and such husband or his relative shall be deemed to have caused her death. It may be noticed that punishment for the offence of dowry death under Section 304-B is imprisonment of not less than 7 years, which may extend to imprisonment for life. Unlike under Section 498A IPC, husband or relative of husband of a woman subjecting her to cruelty shall be liable for imprisonment for a term which may extend to three years and shall also be liable to fine. Normally, in a criminal case the accused can be punished for an offence on establishment of commission of that offence on the basis of evidence, maybe direct or circumstantial or both. But in case of an offence under Section 304-B IPC, an exception is made by deeming provision as to nature of death as dowry death and that the husband or his relative, as the case may be, is deemed to have caused such death, even in the absence of evidence to prove these aspects but on proving the existence of the ingredients of the said offence by convincing evidence. Hence, there is need for greater care and caution, that too having regard to the gravity of the punishment prescribed for the said offence, in scrutinizing the evidence and in arriving at the conclusion as to whether all the above mentioned ingredients of the offence are proved by the prosecution. In the case on hand, the learned counsel for the appellant could not dispute that the first two ingredients mentioned above are satisfied.”

The Supreme Court in *Hira Lal & Others vs. State (Govt. of NCT), Delhi*¹⁴³, Clarified Section 304B of Indian Penal Code, 1860 and 113-B of Indian Evidence Act in Context of dowry Death and considered and read the dowry death as 304-B. Dowry death.- (1) Where the death of a woman is caused by any burns or bodily injury or occurs otherwise than under normal circumstances within seven years of her marriage and it is shown that soon before her death she was subjected to cruelty or harassment by her husband or any relative of her husband for, or in connection with, any demand for dowry, such death shall be called dowry death, and such husband or relative shall be deemed to have caused her death. Explanation.-For the purpose of this sub-section, dowry shall have the same meaning as in Section 2 of the Dowry Prohibition

¹⁴³ *Hira Lal & Others vs. State (Govt. of NCT), Delhi* (2003) 8 SCC 80,

Act, 1961 (28 of 1961). (2) Whoever commits dowry death shall be punished with imprisonment for a term which shall not be less than seven years but which may extend to imprisonment for life.

Further held that “The provision has application when death of a woman is caused by any burns or bodily injury or occurs otherwise than under normal circumstances within seven years of her marriage and it is shown that soon before her death she was subjected to cruelty or harassment by her husband or any relatives of her husband for, or in connection with any demand for dowry.”

Section 113-B of the Evidence Act is also applicable for the matter at hand. Both Section 304-B IPC and Section 113-B of the Evidence Act were introduced by Dowry Prohibition (Amendment) Act 43 of 1986 with a vision to battle the increasing risk of dowry deaths. Section 113-B reads as follows:

“113-B: Presumption as to dowry death.-When the question is whether a person has committed the dowry death of a woman and it is shown that soon before her death such woman had been subjected by such person to cruelty or harassment for, or in connection with, any demand for dowry, the Court shall presume that such person had caused the dowry death.”

Judiciary on Acid Attack:

In *Lakshmi v. UOI*¹⁴⁴ In this case an acid attack survivor filed a petition in 2006, requesting that the government devise measures to control the sale of acid and compensate the victim adequately. In 2013, the Supreme Court placed strict restrictions on the selling of acid, in response to an increase in the number of recorded cases of acid attacks against women.

The selling of acid over the counter was also prohibited by the decision. Following the decision, dealers could only sell and market acid after proving their identity and stating the reason for selling/buying the acid. Following the sale, a thorough report was required to be sent to the police. The law also stated that acid should not be marketed to someone under the age of 18.

¹⁴⁴ *Lakshmi v. Union of India* (2014) 4 SCC 427.

CHAPTER 6

CONCLUSION & SUGGESTIONS

6.1 Conclusion:

Gender discrimination occurs in almost every society. Women have been given secondary status to men for generations; they do not have their own identity and are considered as property of the household to which they belong, confined in the house in the name of honour. The perpetrators of crimes against women, on the other hand, are women or are linked to women. Today, women participate in every sector, but the majority of them are confined to their homes, and their contribution to society or nation building is limited to some degree as a result. Their male counterparts rule the world, possessing all of the world's power and pleasure, while women remain alone, uneducated, invisible, and unrewarded for their contributions to the home, society, and country. Due to the patriarchal mindset, today's women face the wrath of men from the moment they are born until they pass.

In our male-dominated society, women have always taken a back seat in some way. Today's women are working to change people's feudal mindsets and achieve gender equality, but they are facing abuse from their family members in the process. If we equate the past to the present, women have come a long way, but they still have a long way to go to achieve gender equality and shift the community's patriarchal mindset.

Modern women have participated in every field, from the civil rights movement to space exploration; every field has been influenced by women's excellence. Women today face a variety of issues, ranging from a lower sex ratio to women being trafficked for the purpose of marriage, from human rights violations to bonded labor, and so on.

Swami Vivekananda, a leader in women's empowerment, once said the soul has no gender; it is neither male nor female. Sex occurs only in the flesh, and a man who wishes to enter the spirit cannot keep sex distinctions at the same time. He also noted that there is no hope for the world's wellbeing unless women's conditions are changed. Women have endured for millennia, and as a result, they have developed endless patience and perseverance.

In modern India, women have been subjected to violence in the home, at work, and in society at large. However, in terms of land law, women have granted equal rights to men, but the government's enforcement of these laws is lacking. Due to patriarchal mentality, government organs such as the legislature, executive, and judiciary have failed to curb violence against women in the past. Since the people who make or enforce these laws come from the same culture that has treated women as second-class citizens, women are now gaining acceptance in society around the world as a result of increased understanding of their rights and their long fight for equal status.

In India, women are compared to cattle. This condition does not only affect rural areas, but also urban areas. The problem that today's men face is that they are unable to change their 18th-century mentality; they are unwilling to give women dignity, protection, or security because of their feudal mindset. In today's world, women are beaten mercilessly for no apparent reason; she was burned alive for not being able to provide dowry to her husband's family; if a woman fails to comply with the society's rotten patriarchal norms, she can face serious consequences without any blame. Despite the fact that there are many laws protecting women's rights, the performance of India's judicial system is not obscured.

The dilemma that women face is that they believe the violence perpetrated against them is justified because of their long history of injustice and suppression. When women are subjected to violence in their families, they feel normal; they are still reliant on men for all, and the irony is that they do not consider such actions of man to be violent. Due to patriarchal mentality, men take pride in punishing women for their faults, and they have seen their elders do so in the building. It is the primary explanation for the disparity in perceptions of crime against women between men and women.

The key explanation why perpetrators of violence against women are free is because of women's silence and failure to report the crime to the authorities. But the authorities, as well as society, are to blame because we have failed to provide adequate protection or instill trust in them; they fear being abused if they report the crime, which is why they have chosen to remain silent.

The explanation for this is that after reporting the crime, the woman is seen in society as having committed a specific type of crime. If a crime was committed against a woman, we immediately assumed she may have assisted the crime or was seeking vengeance, which is why she filed a lawsuit, or we questioned her integrity. When reporting the crime, women have faced a range of obstacles or violence, and the authorities have failed to provide them with sufficient protection and security. In cases where a family member or relative has committed a crime against a woman, the family can force her to retract her statement or withdraw her complaint. If we are to address the issue of rising crime against women, we must work together as a community to address the evil of gender inequality. To solve the problem and provide equal status to women, we must consider all aspects, including social, political, economic, and other factors that contribute to crime against women.

The man has no idea how much pain and hardship women go through when doing household chores. They believe that it is women's responsibility to fulfill their every desire and to complete their daily tasks at home. The discomfort that women experience in their reproductive roles is not recognized by men. The tasks that women perform while performing various roles in society do not pay them any money. As a result, they are not considered economically active in society or in nation-building.

Women in India must come out in the open, challenge gender bias against them, and lead a social transformation that improves their status and health in society while also combating the patriarchal mindset. We may say that as time goes by, women's conditions will change, and they will be given the most cherished human rights, such as the freedom and equality to make choices and compete with their male counterparts, as well as a good working atmosphere.

In India, the judiciary has played a critical role in combating violence against women. The Supreme Court has issued crucial guidelines and directives aimed at protecting women's rights and putting them on an equal footing with men. The Supreme Court has slammed the executive for failing to follow guidelines and has demanded a full reform of the system in order to reduce violence against women and to give maximum sentences, including capital punishment, to offenders in order to prevent others from committing crimes against women.

Women-oriented policies have been passed by the legislature, which would help to reduce crime against women. Successful police enforcement and a better awareness of women's rights will help to reduce crime against women.

There have been reports of female foetuses found in drains, dug from dry wells, floating in lakes, or eaten by dogs, and stories of women trafficked for marriage and the emergence of polyandry in Hindu society. The gang rape of women in such a way that it shook the entire nation's conscience to satisfy their lust and take the lives of women in order to maintain the so-called honor of the family if they chooses to marry of their own choice.

As citizens of this country, it is our responsibility to ensure that women are respected and protected. Amending and enacting new legislation will not reduce crime against women; the only way to reduce crime against women is for society to offer gender neutral equality to all human beings, and we must educate our future generations about this and provide an atmosphere where they will not have to accept crime against women and will speak out against it.

We have enough laws for women's protection that, if effectively enforced, have the power to uphold law and order in society and punish offenders who commit crimes. However, in order to keep up with the rest of the world or due to the country's shifting socioeconomic fabric, we must improve current laws to keep up with the times. To provide prompt justice to the people and avoid its abuse, we must make a few systematic improvements to the legal system and its facilities, and we must strengthen the efficiency of the lower judiciary to do so.

To maintain the rule of law, we must ensure that our police officers operate in a safer atmosphere and that law enforcement agencies are not subjected to political interference or influence that would negatively impact their efficiency. Transparency in the workings of government offices and departments is important in carrying out public duties, as is accountability for their work. Every state in India has agreed to establish a women's police station in each district, following government directives. The women's police station will be staffed entirely by women and will focus on crimes against women. It is commendable of the government to have a secure atmosphere in which to file complaints against offenders.

According to the National Crime Record Bureau's statistics from, there hasn't been much progress since the Nirbhaya Case.

Women's crimes are a problem in every state in India. Despite legislative changes and the implementation of security measures in public transportation, things have not changed. The only take away from the Nirbhaya incident is that women are more willing to report crimes against them because they are more conscious of their rights and determined to battle for them. However, we also have a long way to go and more work to do in the areas of police reforms, law reforms, harsh sentencing, educational reforms, rape crisis centers, therapy, and public transportation protection to ensure women's safety.

In the last decade, India has made significant progress in terms of economic growth. Female literacy rates have increased from 54 percent in 2001 to 65 percent in 2011, and the maternal mortality ratio has improved from 327 in 2001 to 178 in 2012, indicating a trend toward greater gender equality in the region. The 2011 census, however, revealed that the child sex ratio had fallen to its lowest level since independence, with 914 females for every 1,000 males, demonstrating the boy preference that has persisted. Surprisingly, socioeconomic development alone has little impact on this pattern. Even states with high HDI scores have a low child-to-adult ratio and a high female infant mortality rate. India also falls short of international norms in other areas of gender equality, such as education, workforce engagement, and inclusion of women in public bodies. In the United Nations Development Programmes gender disparity ranking, it ranks 136th out of 186 countries. Women's violence, whether sexual or physical – wife beating is commonly discussed but seldom mentioned – is an expression of male-female power imbalance. It appears to be linked to other indices of gender inequality. The victims' behaviors can also be blamed for the low reporting rate of domestic abuse. According to the National Family Health Survey 3 (NFHS-3), 41% of women believe their husbands are justified in slapping them, and 35% believe a brutal beating is justified if they neglect household chores or child care.

According to the annual National Crime Record Bureau's Crime in India 2019 report, crimes against women increased by 7.3 percent from 2018 to 2019. Uttar Pradesh had the largest number of cases in both groups in terms of absolute numbers. However, Assam had the highest rate (per lakh population) of crimes against women, while Rajasthan had the highest rate of crimes against Scheduled Castes. In 2019, a total of 4,05,861 cases of crime against women were

recorded, up 7.3 percent from the previous year (3,78,236 cases). The most common crime against women under the IPC was cruelty by husband or his family' (30.9%), followed by assault on women with intent to offend her modesty (21.8%), kidnapping & abduction of women (17.9%), and rape (15.9%). According to the NCRB survey, the crime rate per lakh woman population is 62.4 in 2019, up from 58.8 in 2018. The state of Uttar Pradesh had the largest number of crimes against women (59,853), accounting for 14.7% of all cases in the region. Rajasthan (41,550 cases; 10.2%) and Maharashtra (41,550 cases; 10.2%) came in second and third, respectively (37,144 cases; 9.2 per cent). With a rate of 177.8 per lakh people, Assam has the highest rate of crime against women, followed by Rajasthan (110.4) and Haryana (108.5).

Rajasthan had the most rapes (5,997), followed by Uttar Pradesh (3,065) and Madhya Pradesh (2,485). Rajasthan had the highest rate of rape cases, with 15.9 cases per lakh population, followed by Kerala (11.1), and Haryana (10.1). With 7,444 cases under the POCSO Act, Uttar Pradesh had the highest number of crimes against girl girls, followed by Maharashtra (6,402) and MP (6,053). Sikkim (27.1 per lakh population), MP (15.1), and Haryana had the highest rates of these crimes (14.6).

The state with the most dowry cases (2,410) and a rate of 2.2 (per lakh population) was Uttar Pradesh, followed by Bihar (1,120). In 2019, 150 acid attacks were recorded, with 42 in Uttar Pradesh and 36 in West Bengal, according to the survey. According to the study, which spans three volumes and over 1,500 pages, a total of 45,935 cases of crime against Scheduled Castes (SCs) were recorded in 2018, up 7.3 percent from 2018. (42,793 cases).

Crime rate registered showed an increase from 21.2 (per lakh population) in 2018 to 22.8 in 2019. Crime head-wise cases revealed that simple hurt with 28.9% (13,273 cases) formed the largest chunk of cases of crimes/ atrocities against Scheduled Castes during 2019. It was followed by cases under SC/ST (Prevention of Atrocities) Act with 9.0% (4,129 cases), and cases under rape with 7.6% (3,486 cases) as per the report.

UP reported the most cases against Scheduled Castes – 11,829 cases, accounting for 25.8 per cent of the cases across the country. It was followed by Rajasthan (6,794 cases; 14.8 per cent) and Bihar (6,544; 14.2 per cent). However, the rate of such cases was highest in Rajasthan at 55.6 (per lakh population), followed by MP (46.7) and Bihar (39.5). Rajasthan also had the

highest number of rapes against Dalit women (554), followed by UP (537) and MP (510). The rate of rape against Dalit women was highest in Kerala at 4.6 (per lakh population), followed by MP (4.5) and Rajasthan (4.5).

Popular cinema's depiction of social themes could be viewed as a representation of popular societal attitudes. Until the mid-2000s, kissing was not permitted on-screen in Indian cinema due to modesty. Rape or izzat lootna (dishonoring) of women, on the other hand, has been a recurring theme and sub-theme in mainstream Bollywood cinema for decades, with films like *Insaaf Ka Tarazu* and, more recently, *Woh Lamhe* as examples. Many films use rape and the resulting avenging of rape as a central theme. Rape is often used as a subplot to emphasize male actors' heroic roles in films. The common depiction of rape and sexual harassment of women in film, albeit subtly, is shocking in terms of its lack of censorship (as opposed to censorship of activities such as kissing, for example) and its pervasiveness in a mainstream medium of entertainment. This is not to dismiss the minimal yet believable depictions of rape and other forms of sexual assault in films like *Bandit Queen* (Shekhar Kapur, 1994) and *Monsoon Wedding*, which used the film medium to bring the issues into the mainstream. The *saas-bahu* serials (mother-in-law and daughter-in-law soaps) are another type of mass media that has been blamed for highlighting other types of abuse and prejudice in Indian households. At a time when the world is reflecting on its treatment of women, it's important to remember that sexual harassment in the mass media can serve as a means of highlighting issues of violence against women while also serving as an echo of societal stereotypes. While the prevalence and acceptance of violence against women in India's mass media requires further investigation, its existence as a result of societal attitudes is undeniable.

A newlywed couple on their way home is assaulted by a group of young men in the 1978 film *Ghar* (drinking, driving a car and listening to music). The wife has been kidnapped and raped. Aside from the rest of the film/script, the 3 minute sequence from 1978 may be considered representative of society today. The representation of the woman is important to remember. Since she was (a) married and (b) walking with her husband when she was assaulted, she is depicted as an honorable or virtuous individual. The rapists, on the other hand, were portrayed as self-indulgent young men out to have a nice time in a car while under the influence of alcohol.

Although comprehensive legislation is necessary to resolve this problem, legislation is not the only solution. The efficacy of these laws is determined by women's knowledge of them, as well as their willingness and comfort in using them when necessary. Raising legal awareness among women is a critical step toward increasing rape reporting rates. The government must allocate sufficient funds to construct the required infrastructure and ensure the enactment of this law by skilled and trained staff. While the amendment to criminal law states that all rape cases should be prosecuted in fast-track courts and that the trial should be concluded within two months, achieving the required conviction rate would be exceedingly difficult without the requisite judicial changes and resources in place. According to statistics from the NCRB, 83.6 percent of cases are still pending in courts across the country. Also the strictest laws are made ineffective due to this low conviction rate.

The Indian government failed to implement several key recommendations made by a three-member committee created to amend the criminal law, the most relevant of which was the criminalization of marital sexual harassment. According to a 2005 study from the National Family Health Survey, 9% of all women aged 15–49 have witnessed sexual harassment at some point in their lives. 87.5 percent of these women said their current husband was the perpetrator. With over 104 countries around the world outlawing marital rape, it is only natural for India to follow suit without blaming tradition or the institution of marriage.

We all come across different aspects of this topic as health practitioners (doctors, nurses, and public health professionals). Health professionals' understanding of this social issue is an integral aspect of the solution, whether it's an out-patient experience with a survivor of domestic abuse who has non-specific grievances or post-rape treatment of a victim at a primary care facility. Rape has a wide range of public health ramifications. Sexual abuse has far-reaching consequences that affect not just the victim, but also the victim's family and culture as a whole.

Primary care/emergency medical personnel, who may be the first point of contact with these victims, should be able to recognize symptoms of sexual harassment and report them to the proper authorities. It is important to educate these individuals not only in medical care but also in offering psychosocial help to these victims. To integrate regular screening for violence into clinical practice, healthcare practitioners must be tested for their readiness to handle such

patients, and they must be educated in maintaining confidentiality, positive attitudes, and respect for patients' rights.

The provision of medical and legal assistance to victims at their first point of contact after an incident has been shown to improve the rate of reporting and prosecution of these crimes. The first point of contact should ensure that the patients receive emergency contraceptive pills (ECP) or post-exposure prophylaxis (PEP), since these are urgent interventions that are most successful during the first 72 hours after the incident. It is important to develop and train both police and medical staff on standardized procedures in post-rape treatment.

In any criminal case, the forensic evidence plays a significant role in the outcome. The rape conviction rate, which currently stands at 16 percent in all cases, can be increased by careful forensic sample selection and transmission to the appropriate authorities. Every medical officer in the public health system should be qualified to conduct physical examinations and meticulously keep medical records. They should be skilled in collecting forensic evidence from victims' samples and assisting the police and other authorities in providing evidence. To accomplish these goals, public health practitioners should conduct advocacy programs on the best post-rape treatment.

6.2 Suggestions:

Despite many constitutional protections and the passage of women-friendly legislation, violence against women has not decreased significantly. During her research on the theme and reading about the laws and factors that contribute to crime against women, the researcher suggests the following steps to combat the problem:

Women today have proven themselves in every field of existence. They excelled in every area and overcame every obstacle in order to realize their dream. She has performed every role in life that is expected of her in order to achieve equality with men; in the eyes of the law, she is equal, but the crime against her proves otherwise. The society's feudal mindset does not regard her equally to her counterpart. Women are not protected everywhere, from home to work or anywhere else; they are victims of male abuse. Women are entitled to equality in all aspects of life. We will never have a civilized world unless and until we give women equal status and our patriarchal thinking becomes gender neutral. Women in all walks of life must have equal

opportunities in order for India to advance. Women must be treated equally and their interests must be respected at all levels of government.

The law requiring all marriages solemnized in the country to be registered in the marriage registrar office has already been passed, but the law's enforcement is lacking; there is no punishment prescribed by the law for couples who do not register their marriage. Couples who do not report their marriage should face penalties as well as retribution.

The criminal justice system's administration should be overhauled. In India, the police are insensitive to sexual crime victims because they have the same patriarchal mindset. However, as an official, they must follow the rule of law without being manipulated by others, including politicians and their superiors. An effective mechanism will have to be built in order to respond quickly to crimes against women. While the Supreme Court has issued some guidelines, their enforcement is still pending. Police officers should be held accountable and held to deadlines for their work in order to regain citizen's confidence. An impartial oversight body is required to ensure that the police are carrying out their legal obligations and responsibilities. This is important in order to strengthen the public-police relationship. There should be a police complaint authority where citizens may file charges against errant officers who fail to perform their duties, and their misconduct should be monitored separately in all cases or complaints. We must work for the transformation of the police department to ensure that citizens feel free to contact officers and file complaints. Fundamental rights granted to citizens of this country can only be protected if the country's police force is successful. The police force must be customer-oriented, dealing with citizens efficiently and scientifically, and quickly resolving their complaints. To eliminate gender inequality, the police department will collaborate with the city. More women in the police force are required, as are volunteers from the public or community who have been trained to perform their civic duties.

To cope with the backlog of lawsuits, the number of courts in our country needs to be increased. With a systemic improvement in infrastructure, the burden of arrears in courts would be reduced by half, resulting in delays in implementing the law of the land. To should the backlog and provide swift justice to the aggrieved, the Judge's power must be increased. The lower courts should not use the old-fashioned form of delivering justice; instead, they should follow the apex court's directions for expeditious case resolution.

In Indian culture, a sexual offense has always been seen as a stigma that women have to deal with. We need to improve the way people think of victims in society. When a woman raises her voice against someone who has committed a crime against her, she considers the society and she is concerned about being labeled as a co-conspirator in the crime. It takes bravery to report a crime against her in front of the authorities and society; rather than applauding her decision, we prefer to disgrace her and form our own opinions about her. We must clearly establish that the only one who suffers from these crimes is the perpetrator, not the victim. We must reassure the victims that they have done nothing wrong in reporting these crimes, and we must encourage women to stand tall in society. We must ensure that they are able to discuss crimes such as rape and sexual assault in the same way as they discuss other crimes such as murder and robbery. In today's media, specific and impartial reporting of these crimes is needed. We must erase guilt from the victims' minds, leaving them with only the physical nature of the crime to worry about. We must shift society's attitude toward victims of such crimes so that women feel safe and confident in reporting crimes against them, and more offenders will be punished. We must eliminate the stigma associated with sexual offenses. We must provide a safe space for women to speak out about sexual offenses committed against them, rather than a feudal culture that views sexual offenses and their victims with disdain.

To enhance the status of women, it is essential that all women's laws be uniform. Except for caste, creed, and religion, we need a uniform rule. There is no uniformity in personal law, which contributes to the abuse of women by men acting on instinct. The Uniform Civil Code aims to modernize personal laws concerning land, marriage, divorce, child support, adoption, and inheritance. The Uniform Civil Code is urgently needed, and the current administration is working hard to gain the support of all parties and citizens who will be influenced by it.

Muslims, especially Muslim women, have suffered as a result of the lack of a Uniform Civil Code, according to retired Supreme Court Justice Markendey Katju.

Current laws that deprive women of all sorts of rights over their lives, land, careers, and other aspects of their lives must be modified in order to provide women with a life of choice and dignity.

To stop the evil of so-called justice courts (Khap Panchayat) killing young men and women in the name of honour when they want to marry according to their own desires, we need a clear law that deals with this type of crime. The Supreme Court has issued stern judgments in an attempt to stop this violence, but the people continue to commit honor killings at an alarming rate. The Indian Law Commission has also recommended that a law be passed to curb honor killings in its report.

In India, elevating women's status entails making them self-sufficient and economically independent. When it comes to the government's macroeconomic agenda, women are not treated equally. Women may not have an abundance of wealth, and society does not provide them with as much as they deserve, but they still strive to compete with men in every sphere. When we consider the regular work hours that she has to work, they do more work than men. However, we are unable to provide or translate this information into money or accounts. We must provide women with equality, but this can only be accomplished after they have achieved economic independence.

In India, education is the only way to improve women's status. We will break the chains of exclusion and narrowmindedness if the children of this world, both boys and girls, have equal access to education and we are able to teach them about gender equality and respect for women. As a result, when they are young, they will be able to recognize their rights, respect women, and not discriminate based on gender. Women are able to protect themselves independently as a result of their education. We must ensure that education reaches every corner of India, and education policy must be updated to ensure that new books provide material that is equitable for men and women. To free women from the shackles of discrimination, achieve gender equality, and gain respect in society, India's education system requires change. It will take a long time, but if we are to achieve gender equality and boost women's status, we must ensure that every child in this country receives an education.

In India, there are only two ways to combat the evil of prostitution. To begin with, we have enough rules, but their implementation is lacking. Even though there are several laws in effect, the government has struggled to regulate human trafficking and prostitution. The government has the ability to significantly reduce the trafficking and abuse of prostitutes, and sex workers should be included in national health programs. The second step is to make the sex

trade legal in India. It is very difficult to combat this crime because it is considered the world's oldest occupation, dating back to the dawn of time.

However, if we legalize this trade, we will be able to regulate it, as well as rehabilitate and treat those who are involved in it. It will aid in the prevention in human trafficking of women.

India, on the other hand, has a vibrant culture as well as religious and social values. So, before we legalize this exchange, we need to fix people's fears. The NGOs are doing an excellent job of rehabilitating sex workers and their children, as well as providing them with medical care. However, the government should establish a department dedicated to women's recovery, therapy, medical assistance, legal awareness, and trafficking and forced prostitution.

In today's world, the Vishaka Guidelines and Factories Act of 1948 are not completely enforced. The guidelines to provide protection to working women in factories, BPOs, LPOs, and other institutions, the regulations about sending a security guard with female workers, CCTV cameras, and GPRS in vehicles are not enforced in MNCs/BPOs, etc., leaving women vulnerable to crime at night. The authorities should ensure that any establishment in India complies with the Apex Court's orders as well as the Factory Act of 1948. If any establishment/factory/MNC/BPO/LPO/etc. does not follow the directions and rules of the Factory Act and the Apex Court, they should face harsher penalties.

In India, the idea of living in relationship is relatively new. This idea has been legalized by the Supreme Court, which stated that it is well within their right to life and cannot be considered a criminal offense. But the argument is that India as a culture has not approved of this premarital relationship and has labeled it a sin. There is no doubt that we, as a society, have our own reservations about this new idea. The woman in this relationship is vulnerable to a variety of forms of abuse, but we lack legislation that explicitly addresses this issue; there is too much uncertainty about whether to regard them as husband and wife or what the status of children born from a live-in relationship is. Except for the judgments of the supreme courts, there is no clear rule. However, specific laws or specific Directions and Guidelines should be in place to address live-in relationships and the problems that arise as a result.

The Government has to open Legal Aid Clinic, Legal Seminars and other programmes in urban as well as rural areas to aware them about their rights. These programmes are designed specifically for woman, so they are more aware about their rights and if there is any violation of their rights then they can report them to appropriate authorities. We should have these programmes in every village of India time and again to educate woman about their rights.

The Section 497 of Indian Penal Code which deals with adultery should be amended to give women right to file a suit against the adulterous husbands.

The specific laws on adjournment should be amended to make sure that case doesn't get linger on one pretext or another and it becomes a tool in the hand of accused. The case has to be finished in particular time period. There should be law to prevent frivolous cases which are only with intent to harass the other party. For example cases related to section 498-A IPC. The Apex Court has also shown its apprehension over such cases. Person who files such cases should be punished severely, so the faith in justice can be restored.

Rape crisis center should be established in every Government Hospital. There should be counseling of rape victims on the expense of government. So the women can come out of trauma of this heinous crime and can live happily in the society.

The Sexual offence has to dealt by the women police officer as the women feel comfortable in front of women police officer, and the case related to these sexual has to be heard by women judge in fast track court so the justice can be provided to them by giving them favorable environment where they can record their statement and prove their case.

As suggested by Justice J.S Verma Committee that to provide safety to women there has to sufficient public transport in day and night and at night every transport vehicle has a security guard. There has to be identity card for each and every person working and they can only ply the vehicle. The vehicle should have its light on in the night.

As suggested by Justice J.S Verma Committee a special procedure for protecting persons with disabilities from rape, and requisite procedures for access to justice for such persons is also an urgent need. Amendments to the Code of Criminal Procedure, which are necessary, have been suggested. The protocols for medical examination of victims of sexual

assault have also been suggested, which we have prepared on the basis of the best practices as advised by global experts in the fields of gynecology and psychology. Such protocol based, professional medical examination is imperative for uniform practice and implementation.

There should be no dark corner in the streets of this country. Every dark spot or street should have street light installed. There should be multiple PCR vans which have women police officer on board to provide safety as the dark spots in nights are more prone to facilitate the crime. All the public vehicle and commercial taxis should have GPS tracker in them so they can be tracked in case of crime and the police should have details of the entire persons driving these vehicles.

The Nirbhaya Fund should be utilized for the rehabilitation of victims of sexual offences which includes acid attack. The victims compensation should be provided to them at the earliest, the fund should also be utilized for the upliftment of women in society their rehabilitation, medical aid and counseling is done by the government.

When taking down accusations of crimes against women, police officers must be extremely cautious. They must follow the rules and procedures when recording the specifics of both the violence against the women and the crimes committed by the defendant. The police must keep a comprehensive offender's file, with information on the number of offences registered, the actions taken, how many of them were eventually brought in court, and the results of such cases, among other things.

Independent systems must be built to look into the ground situations of the respective sites, in addition to the generic version of submitting complaints to the police. If the procedure operates on existing biases, does not report grievances because there is a power struggle between the parties, harasses victims' families, and so on, the officials concerned should be punished for their actions. Any explicit and consistent rules must be formed so that the police can investigate certain cases of crimes against women more objectively, and so that the police can determine what actually qualifies as a crime against women. Police officers must be educated on how to respond to incidents of violence against women, how to collect reports, how to investigate the matter, how to react to sensitive cases, how to collect and retain evidence, and how to clarify the types of rights and safeguards available to the victims and their families.

The laws in India are plenty but we are not able to implement our laws effectively, the laws promises women security but due to their poor implementation, the perpetrators use the lacunas of laws and get away with crime. However, due to the tiring long judicial procedure women can't able to stand for long in the wait for justice and hope that this condition will improve in future. So effective implementation of all these laws is the foremost requirement of the hour.

In the last two decades, all forms of violence against women have become more widely recognized. It's also seen as a significant issue on a national and international level that needs to be addressed right away. As it happens between close relatives in the safety of their homes, archaic attitudes toward women around the world contribute to the abuse, which has been ignored or condoned.

Today, we have international conventions, treaties, international, regional, and national legislation, among other things, that provide us with a variety of rights and protective measures for women who are victims of abuse, such as domestic violence and other heinous crimes. In all of these efforts, progress in achieving women's rights has been slow all over the world. The various international, regional, and national conventions on women encourage governments from all over the world, as well as research agencies, non-governmental organizations, and other groups, to support research on the prevalence of domestic violence, as well as its causes and consequences. It also aids in determining the efficacy of legislation and provides victims with preventative steps.

IWRAW Asia Pacific acknowledges that the CEDAW Convention was a product of its time, and that if such a convention were drafted today, violence against women would be expressly acknowledged and published, most likely in some detail. It also addresses CEDAW's General recommendation 19, which is outdated, despite the Committee's ability to improve its interpretation of the roles and duties in its other General recommendations and practice.

IWRAW Asia Pacific also recognizes that much work remains to be done to alleviate the effects of GBVAW, and that stronger international (legal) interventions will help greatly in this effort. The question remains as to how any new policies that could be implemented should be handled, both boldly and cautiously. The crucial question is how to better ensure that the

Convention's principles and instruments, as well as other equality assurances, are implemented at both the international and national levels. IWRAW Asia Pacific also believes that any discussion of a new convention should consider what has already been accomplished while carefully considering the possible benefits and drawbacks of pressing for a new convention.

Many countries have laws prohibiting violence against women, the most popular of which is domestic violence. In India, for example, the Indian Penal Code specifies punishments for crimes against women. Some countries have strict domestic abuse legislation, while others are enacting new legislation or amending existing laws to cover crimes against women. However, it is often assumed that these laws and policies are inadequate to eliminate the world's violence crisis.

Finally, women-centric offenses are not merely a legal issue that can be addressed with the appropriate legal remedies. It's also a social and psychological issue that can be solved by making radical changes in culture and in how women and children are handled. Although sanctions aim to relieve the symptoms of crimes against women, they can only go so far in addressing the root causes. In reality, despite numerous international human rights instruments and remarkable economic, technical, and social progress that focuses on closing gender gaps, millions of women around the world are systematically violated and subjected to various forms of violence, a tragic crime that must be recognized and vigorously addressed.

**APPLICATION OF MOST-FAVOURED NATION PRINCIPLE TO
DISPUTE SETTLEMENT**

**Dissertation Submitted In Partial Fulfillment Of The Academic
Requirement Of Master of Laws (LL.M) In (Criminology)**

AT

AMITY UNIVERSITY, RAJASTHAN

SUBMITTED BY

RAHUL SHARMA

A215104520026

UNDER THE SUPERVISION OF

ASSISTANT PROFESSOR

MR.PRATEEK DEOL



ACKNOWLEDGEMENT

I Rahul Sharma would like to express my special thanks of gratitude to my faculty Mr PRATEEK DEOL who gave me the golden opportunity to do this wonderful dissertation on the topic “Application of most- favoured nation principle to dispute settlement” also helped me in doing a lot of Research and I came to know about so many new things I am really thankful to her. I would also like to thank my parents and friends who helped me a lot in finalizing this dissertation within the limited time frame.

RAHUL SHARMA

LL.M. (Criminology)

2nd semester

Date:

CERTIFICATE

This is to certify that the dissertation entitled, "APPLICATION ON MOST FAVOURED NATION PRINCIPLE TO DISPUTE SETTLEMENT BODY" submitted by Rahul Sharma in partial fulfillment of the requirements of the dissertation for II Semester of Amity Law School and is an authentic work carried out by him under my supervision and guidance.

Mr. Prateek deol

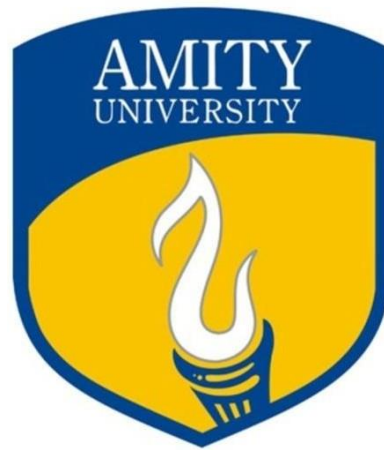
Assistant Professor

Amity University Rajasthan

Date:

SYNOPSIS

Paving a New Ground of Harassment: An Analysis of
Misuse of protection Laws in India



AT
AMITY LAW SCHOOL
AMITY UNIVERSITY RAJASTHAN
JAIPUR

SUBMITTED BY

Name -Rajarshi Mehta

LLM – Criminal Law (2020-21)

SUBMITTED TO

Mr. VEDANSH SHARMA

Assistant Professor

Candidate declaration

I the undersigned solemnly declare that the Dissertation is based on my own work carried out during the course of our study under the supervision of. I assert the statements made and conclusions drawn are an outcome of my research work. I further certify that . The work contained in the dissertation is original and has been done by me under the general supervision of my supervisor. The work has not been submitted to any other Institution for any other degree/diploma/certificate in this university or any other University of India or abroad. We have followed the guidelines provided by the university in writing the report. Whenever we have used materials (data, theoretical analysis, and text) from other sources, we have given due credit to them in the text of the report and giving their details in the references.

Name – Rajarshi Mehta

LLM Criminal Law

Supervisor certificate

This is to certify that the work contained in the Dissertation entitled “Paving a New Ground of Harassment: An Analysis of Misuse of protection Laws in India”, submitted by Rajarshi Mehta Enrolment NoA215104520007 for the award of the degree of LLM to the Amity University Jaipur, is a record of Bonafede research works carried out by him under my direct supervision and guidance. I considered that the thesis has reached the standards and fulfilling the requirements of the rules and regulations relating to the nature of the degree. The contents embodied in the thesis have not been submitted for the award of any other degree or diploma in this or any other university.

Date:10th May 2021

Signature

Place:

(Supervisor)

**PROS & CONS OF MEDIA TRIAL IN INDIA WITH SPECIFIC REFERNCE TO
VICTIM'S PRIVACY**

Dissertation Submitted in Partial Fulfillment of the Academic Requirement for the Award of
Degree of **Master of Laws**

(LL.M.) in (Criminal Law)

At

AMITY LAW SCHOOL

AMITY UNIVERSITY RAJASTHAN

JAIPUR

BATCH 2020-2021



SUBMITTED BY:

RAJAT SINGHAL

LL.M. (CRIMINAL LAW)

A215104520008

2nd SEMESTER

SUBMITTED TO:

DR. VINOD KUMAR

ASSOCIATE PROFESSOR

AMITY LAW SCHOOL

DECLARATION

I, **RAJAT SINGHAL** student of **LL.M. (Criminal Law) 2nd Semester**, Enrollment No. **A215104520008**, declare that this Dissertation & the work presented in it is original & has been generated by me as the result of my own original research.

PROS & CONS OF MEDIA TRIAL IN INDIA WITH SPECIFIC REFERNCE TO VICTIM'S PRIVACY

I confirm that:

- This work was done wholly or mainly while in candidature for a professional degree at this college;
- Where any part of this dissertation has previously been submitted for a degree or any other qualification at this University or any other institution; this has been clearly stated;
- Where I have consulted the published work of others, this is always clearly attributed;
- Where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my own work;
- I have acknowledged all main sources of help;
- Where the thesis is based on work done by myself jointly with others; I have made clear exactly what was done by others & what I have contributed myself.

RAJAT SINGHAL

LL.M. (Criminal Law)

AMITY LAW SCHOOL

DATED: 28.04.2021



AMITY
UNIVERSITY
— JAIPUR —

CERTIFICATE

This is to certify that the Dissertation entitled **PROS & CONS OF MEDIA TRIAL IN INDIA WITH SPECIFIC REFERNCE TO VICTIM'S PRIVACY** is a bonafide record of independent research work done by **RAJAT SINGHAL** (Enrollment No. **A215104520008**) under my supervision & submitted to **Amity Law School** in partial fulfillment of the Academic Requirement for the award of the Degree of **Master of Laws (LL.M.) in (Criminal Law)** At **AMITY LAW SCHOOL, AMITY UNIVERSITY RAJASTHAN, JAIPUR.**

Further certify that work is perfect for submission & evaluation.

I wish him all the success in life.

Dr. Vinod Kumar

Associate Professor

AMITY LAW SCHOOL

**JUDICIAL ACTIVISM : IMPACT OF INDIA'S JUSTICE
DELIVERY SYSTEM ON COMMON MAN**

Dissertation Submitted in Partial Fulfilment of the Academic Requirement of
Degree of Master of Laws (LL.M) in (Criminal Law)



At Amity University Jaipur, Rajasthan
SP-1 Kant Kalwar, NH11C, RIICO Industrial Area,
Jaipur, Rajasthan 303007

SUBMITTED BY:

SHASHWAT DHANKHAR

LLM 2ND SEMESTER

CRIMINAL LAW

2020-2021

UNDER THE SUPERVISION OF

Dr. VINOD KUMAR

(Associate Professor)

Amity Law School



The Report is Generated by DrillBit Plagiarism Detection Software

Submission Information

Author Name	shaswat
Title	dhankar
Submission/Paper ID	305150
Submission Date	17-Jun-2021 02:51:28
Total Pages	108
Total Words	42550

Result Information

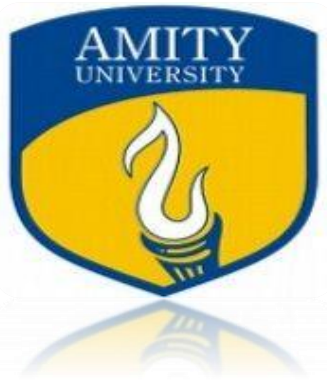
Similarity	12 %
Unique	88 %
Internet Sources	1 %
Journal/Publication Sources	8 %
Student papers	2 %
Total content under 'References'	2 %
Total content under 'Quotes'	2 %

Exclude Information

References/Bibliography	Excluded
Quotes	Not Excluded

RESEARCH DISSERTATION
ON
RIGHT OF ACCUSED PERSON WITH SPECIAL
REFERENCE OF BAIL

Submitted for the partial fulfillment of the award of
Degree of LL.M IN CRIMINAL LAW



CRIMINAL LAW

SUBMITTED BY:

SURENDRA SANGWA

A21510520024

Surendra.sangwa1@student.amity.edu

SUBMITTED TO:

Mr. KESHVA JHA

Supervisor in Charge

CRIMINAL LAW

AMITY LAW SCHOOL, JAIPUR

ACKNOWLEDGEMENT

Writing this dissertation has been an intense learning experience for me, not only in the legal arena, but also on a personal level. I would like to thank all the people who have supported and helped me so much throughout this period.

First of all I would like to offer my hearty devotion to the almighty without whose blessings this research dissertation would not have been accomplished.

I express my sincere gratitude to Mr. KESHAV JHA for his continuous guidance, advice and support in the dissertation research, for his relaxation with respect to the time deadlines which provided us to research in a better and in an effective way. I could not have imagined having a better faculty to work with as I learned to work hard during this whole practice. I extend my gratitude to all my other friends and colleagues for their continuous suggestions and constructive criticisms.

Finally, I would express my deep gratitude to my parents for their love, understanding, and inspiration. Without their encouragement and blessings, I would not have been able to finish this work.

- SURENDRA SANGWA

CERTIFICATE

This is to certify that, Ms. Surendra Sangwa, student of 2nd semester, LL.M(CRIMINAL LAW), Amity Law School has submitted his dissertation titled “*RIGHT OF AN ACCUSED PERSON WITH SPEIAL REFERENCE TO AIL*” for partial fulfillment of the requirements for the award of degree of “MASTER OF LAW (CRIMINAL LAW)”, LL.M from Amity University Rajasthan under my supervision & guidance. the reserarch is an original piece of research work by him and satisfies the requirement for submission as laid down in the regulation of the Amity University Rajasthan.

Mr. KESHAV JHA

(Faculty for Criminal Law)

AMITY LAW SCHOOL, JAIPUR

AMITY UNIVERSITY RAJASTHAN , JAIPUR

Crimes against Women with special reference to Rape Laws in India

**Dissertation submitted in Partial Fulfilment of the Academic Requirement of Degree of
Masters of Laws (LL.M) in Criminal law**

At

**AMITY LAW SCHOOL
AMITY UNIVERSITY RAJASTHAN
JAIPUR**



SUBMITTED BY:

MS. UROOJ AMIN

LL.M 2nd SEMESTER

(CRIMINAL LAW)

SUPERVISED BY:

DR. VINOD KUMAR

ASSOCIATE PROFESSOR

AMITY LAW SCHOOL

2020-2021

Candidate Declaration

I, **Urooj Amin** hereby declare that the work presented in this dissertation is a genuine work done originally by me under the closer guidance and supervision of **Dr. Vinod Kumar, Associate Professor, Amity Law School, Amity University, Rajasthan**, following the stipulated guidelines and the same report has not been submitted elsewhere for the award of any degree. All sources of information referred in this work are acknowledged with reference to the respective authors.

Urooj Amin

(Degree Candidate)

Certificate of Supervisor

This is to certify that the dissertation entitled, “**Crimes against Women with special reference to Rape Laws in India**”, submitted to Amity University, Rajasthan in fulfillment of the requirements for the award of the degree of LL.M, embodies to the best of my knowledge, a faithful record of original research work carried out by **Ms. Urooj Amin** under my supervision and that this work has not been submitted in part or full for any degree or diploma of Amity University or any other university.

Dr. Vinod Kumar

(Supervisor)



AMITY UNIVERSITY, RAJASTHAN
LLM DISSERTATION
ON
TRAFFICKING OF HUMAN BEINGS: A COMPREHENSIVE STUDY
Dissertation for LLM CRIMINAL LAW

UNDER THE SUPERVISION OF

Mr. KESHAV JHA

(Faculty of Law)

Amity University, Rajasthan

SUBMITTED BY

UTTAM SINGH RANWA

LLM (CRIMINOLOGY)

Enrollment No.-A21504520027

April,2021

Declaration

I, hereby declare that the dissertation entitled “TRAFFICKING OF HUMAN BEINGS: A COMPREHENSIVE STUDY ” is a record of individual and original research work carried out by me under the supervision of Mr. Keshav jha, Faculty of law, Amity University, Rajasthan. The same has not been submitted for the award of any diploma, degree or similar title to any other university.

Date: April, 2021

UTTAM SINGH RANWA

LLM

Enrollment No. A2104520027

Amity University, Rajasthan

CERTIFICATE

This is to certify that the dissertation entitled “**TRAFFICKING OF HUMAN BEINGS: A COMPREHENSIVE STUDY**” has been prepared by UTTAM SINGH RANWA, a student of LLM at Amity University, Rajasthan under my supervision and guidance and I recommend it for submission for the evaluation. The dissertation work is submitted in partial fulfillment of requirements for LLM Degree. The work is comprehensively sufficient and complete to standards of academic.

Date: April, 2021

Supervisor

Mr. Keshav Jha

(Faculty of Law)

Amity University, Rajasthan

Protecting Innocence: Victim Rights of Abused Children in Criminal Justice System
Dissertation submitted in Partial Fulfilment of the Academic Requirement of Degree of
Masters of Laws (LL.M) in Criminal law

At

AMITY LAW SCHOOL
AMITY UNIVERSITY RAJASTHAN
JAIPUR



SUBMITTED BY:

MS. Varsha Singh Choudhary

LL.M 2nd SEMESTER

(CRIMINAL LAW)

SUPERVISED BY:

Mr. Vedansh Sharma

ASSISTANT PROFESSOR

AMITY LAW SCHOOL

2020-2021

Certificate of Supervisor

This is to certify that the dissertation entitled, “**Protecting Innocence: Victim Rights of Abused Children in Criminal Justice System**”, submitted to Amity University, Rajasthan in fulfillment of the requirements for the award of the degree of LL.M, embodies to the best of my knowledge, a faithful record of original research work carried out by **Ms. Varsha Singh Choudhary** under my supervision and that this work has not been submitted in part or full for any degree or diploma of Amity University or any other university.

**Vedansh
Sharma
(Supervisor
)**

Efficacy of Right to Information Act in prevention of corruption

Dissertation Submitted in Partial Fulfillment of the Academic
Requirement of Degree of **Master of Laws (LL.M) in (Criminal Law)**

At
Amity University, Rajasthan

SUBMITTED BY
VIKASH CHAUDHARI
A215104520003

UNDER THE SUPERVISION OF
MR.Shobhitabh Srivastava
Assistant Professor,
Amity Law School,

Amity University, Rajasthan
SP -1, kant kalwar, RIICO Industrial Area, NH- 11C,
Jaipur, Rajasthan 303007



The Report is Generated by DrillBit Plagiarism Detection Software

Submission Information

Author Name	zip9
Title	Zip File
Submission/Paper ID	301643
Submission Date	11-Jun-2021 01:57:15
Total Pages	82
Total Words	25596

Result Information

Similarity	31 %
Unique	69 %
Internet Sources	17 %
Journal/Publication Sources	21 %
Total content under 'References'	1 %
Total content under 'Quotes'	6 %

Exclude Information

References/Bibliography	Excluded
Quotes	Not Excluded

**RIGHTFULNESS OF FIR IN CASES OF SEXUAL
ASSAULT IN INDIA: AN ANALYTICAL STUDY**

Dissertation Submitted in Partial Fulfillment of the Academic Requirement of Degree of
Master of Laws (LL.M) in (Criminal Law)

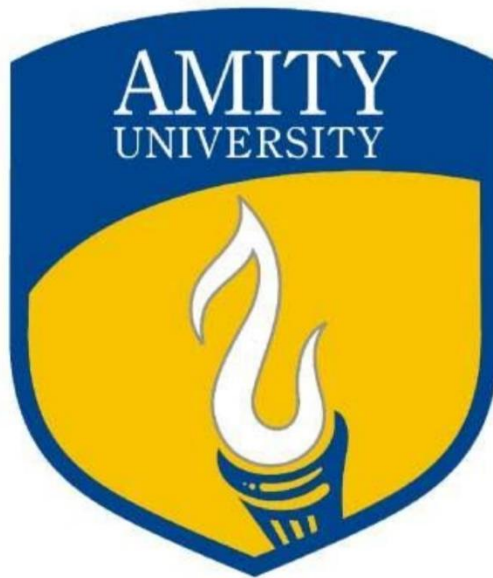
At
Amity Law School, Jaipur

SUBMITTED BY

YASHPAL SINGH RATHORE

UNDER THE SUPERVISION OF

Mr. Keshav jha
Assistant professor



**Amity University Jaipur Campus. SP-1, Kant Kalwar, RIICO Industrial Area, NH-
11C, Jaipur, Rajasthan, 303002**

DECLARATION

This Dissertation titled **Rightfulness of FIR in cases of Sexual Assault in India: An analytical study** submitted to **Amity University Jaipur** for the award of degree of **Master of Law (LL.M.) in subject of Criminal Law** is a result of my own work and effort. Any material scripted by any other author or commentator and used hereinafter has been thoroughly acknowledge.

It has not already been accepted for any degree, and is also not concurrently submitted for any other degree.

Name- Yashpal singh rathore

Enroll no :- A215104519002

Batch- 2020-2021

CERTIFICATE

I have pleasure to certify that **Yashpal singh Rathore** , a student of **Amity Law School, Jaipur** has pursued his research work and prepared the present dissertation titled, (**RIGHTFULNESS OF FIR IN CASES OF SEXUAL ASSAULT IN INDIA: AN ANALYTICAL STUDY**) under my guidance and supervision.

To the best of my knowledge, the present dissertation is the result of her/his own research work.

This is being submitted to **Amity University Jaipur** for the **Degree of Master of Laws (LL.M)** in partial fulfillment of the requirement of the said degree.

Mr. Keshav Jha

Assistant professor

Amity law school

CHAPTER 1

INTRODUCTION

Human beings have been endowed by nature with a mind and brainpower that separates them from other species and places them above all other living creatures in the universe. The advancement of human civilization ultimately led to the discovery and innovation of new technologies, ranging from basic survival needs to modern-day luxuries. Crime, in whatever form it takes, has always had an effect on society, whether directly or indirectly. In today's world, there has been a massive rise in the use of the Internet in every aspect of society, and as a result of this increase, a number of new crimes have emerged. Cyber Crimes are described as crimes that include the use of computers in conjunction with the use of the Internet.

The law that governs computer and Internet technology is known as cyber law. It goes without saying that modern communication technologies and emerging media have radically altered our way of life. Almost everybody is impacted in today's highly digitalized environment. The way people do business is undergoing a revolution. Almost all stock trades are done through a depository. Almost all businesses rely heavily on their computer networks to keep their data in electronic form, and customers use credit cards to shop. The majority of people communicate through e-mail, mobile phones, and SMS messages. Instead of conventional paper records, businesses and consumers are increasingly using computers to create, distribute, and store information in electronic form. Digital signatures and e-contracts are quickly displacing traditional business methods. The industry has seen a quantum leap in consistency, quantity, and pace since the arrival of the computer era. There has been a change in lifestyle. The technology, on the other hand, is still evolving. The human mind is responsible for instilling in people a desire for knowledge and the ability to think, which leads to the development of modern science and technology. Today, the world is witnessing a new age of illegal activity in cyberspace, which is taking place all over the world, regardless of geographical boundaries. These cybercrime actions may be motivated by money, be linked to computer content, or be directed at computer systems' security, honesty, and accessibility. Governments and companies face different levels of risk and danger. Cybercriminals are likely to have a variety of characteristics, including age, sex, socioeconomic background, ethnicity, and motivation. The degree of criminal organization is a distinguishing feature of the human association aspect that drives criminal behavior. India is responsible for nearly \$8

billion of the \$110 billion expense of global cybercrime. The Information Technology (IT) Act of 2000 outlines the types of offenses that are punishable. Social networking has been impacted by cybercrime. A crime reduction strategy with specific objectives and targets should be identified, and the government should include permanent recommendations in its programs and structure for controlling crime, as well as ensure that clear roles and goals for crime prevention are established within government.

Technology and vital infrastructure are at the root of cybercrime. The number of people using the internet is growing all the time, which increases the likelihood of various forms of crimes. Because of technological advancements, the essence of cybercrime is changing. Technology-based crimes are becoming more prevalent by the day, and they must be addressed as soon as possible. These crimes are not limited to computers; they also include other electronic devices such as financial processing machines, telecommunication, and machinery. It is difficult to recognize cyber security concerns due to their diverse existence, which contributes to a lack of knowledge about security issues. With the assistance of the government and non-governmental organizations, we will organize seminars, free ads, and public awareness campaigns. Recognizing cyber world crimes and illiteracy should begin at the grassroots level, with institutes, computer centers, colleges, and individuals. Despite the fact that India has taken several measures to combat cybercrime, the cyber law cannot afford to remain static; it must evolve in tandem with the changing times. By encompassing globalization in all aspects of life, digital technology has taken the true definition of globalization to the entire world. People were able to interact with their loved ones who lived on the other side of the planet thanks to technological advancements. People became more familiar with the word "Cyber" as technology progressed, and the "evolution of Information Technology (IT) gave birth to the cyber space". Since the internet has become one of the biggest advancements in the field of communication, it has begun to provide opportunities for all people to gain access to either information or data storage through the use of internet facilities. With the advent of the internet, it has been rightly said that the entire planet has become a global village.¹

However, this cyber infrastructure has been shown to have two-sided effects: on the one hand, it allows people to connect, and on the other hand, it is being used by cyber criminals to hack others through the Internet and other global communications technologies.

¹ Vanita Bansal, *Cyber Crimes & Its Related Laws*, 2(7) JCIL 1, 2-3 (2016).

Misuse of the internet for the purpose of committing cybercrimes, also known as computer-related crimes, internet-related crimes, or e-crimes, has become widespread in recent years. Cyber-crimes are just real-world crimes carried out through the medium of a machine, so “there is little distinction between identifying a crime in the cyber and real worlds”. Just the crime medium is different. There are no "cyber-borders" between countries, so cybercrime is "universal" or "transnational." Digital crime, cybercrime, e-crime, hi-tech crime, or electronic crimes all apply to illegal activity that takes place in cyberspace and involves the use of a computer or network as a weapon, target, or bystander. Furthermore, in the modern age, cyber-crime is not only a problem for India, but it has also become a concern for the entire world. As a result, the entire world must step forward to address this problem. Due to the global nature and legal issues of cybercrime, so many efforts have been made by two *“international organizations, such as the G-8 Group, OAS (Organization of American States), APEC (Asia-Pacific Economic Cooperation), and the Council of Europe to ensure harmonization of provision in individual countries, but such an approach is found vital in the matters of investigation.”* Because of the nature of cybercrime, a cyber-criminal may commit a crime from anywhere in the world, eliminating the need to travel to the victim's location. Though countries such as India, the United States, and the United Kingdom have passed legislation to deal with such crimes, and the judiciary is also playing an important role, in some cases these are found to be inadequate, which will pose a significant challenge to the national and international judicial systems in the near future. Many attempts are currently being made to create a shared agenda for harmonizing the environment between nations in order to tackle cybercrime through “international treaties, conventions, or commissions, such as the UNCITRAL Model Law.” Despite the existence of many laws aimed at fighting cybercrime, several complex legal problems remain unresolved. It is essential to adopt the “General Assembly's recommendation that the United Nations system should be instrumental in advancing global approaches to combating cybercrime and to procedures for international cooperation, with the aim of preventing and mitigating the negative impact of cybercrime, both for the United States and the United Kingdom.” States should be encouraged to change their criminal legislation as soon as possible to address the unique nature of cybercrime. It is also proposed that, in the case of conventional types of crime committed using emerging technology, those laws that are no longer adequate be clarified or abolished by introducing new provisions for new crimes or upgrading those that are no longer adequate. States should

be encouraged to be motivated by the provisions of the Council of Europe Convention on Cybercrime² when deciding the strength of new legislation.

Cybercrime refers to crimes committed on or across the Internet. A wide range of criminal activities are among them. The term "cybercrime" is a catch-all term that encompasses a wide range of criminal activities. Because of the anonymous existence of the Internet, many troubling activities are taking place in cyberspace, allowing criminals to engage in a variety of illegal activities known as cybercrimes. *“Since technology is the tool used in cybercrime, the perpetrators are typically technically trained individuals who have a comprehensive understanding of the Internet and computer applications. Cyber-stalking, cyber-terrorism, e-mail spoofing, e-mail bombing, cyber pornography, and cyber-defamation are some of the more recent cybercrimes.”* Any traditional crimes can be classified as cybercrimes if they are carried out over the Internet. For example, under the IPC, 1860, stealing, fraud, deception, mischief, misrepresentation, and intimidation are all punishable offenses.

1.1 Meaning & Definition:

The Information Technology Act, 2000:³

As far as the precise concept of cybercrime is concerned, it has yet to be codified in any legislation or regulation. Even the Information Technology Act of 2000 lacks a concept of cybercrime. Cybercrimes, on the other hand, are those types of crimes in which a *“machine is either an object or a subject of actions constituting the offense”*, or both. As a result, cybercrime encompasses any operation that uses a computer as an instrument, target, or means of committing additional crimes.

Prof. S.T. Viswanathan:

He has proposed three different concepts of cybercrime, which are as follows:

- *“Any criminal activity in which a computer is the medium or target of the crime, i.e. any crime whose means or intention is to manipulate a computer's work, Drug trafficking, online gambling, financial fraud or forgery, cyber defamation,*

² European Treaty Series 185 - Cybercrime Convention, 23.XI.2001.

³ The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).

pornography, intellectual property crimes, cyber-stalking, and spoofing are only a few examples of cybercrimes that use computers as a weapon;

- *Any event involving computer technology in which a victim suffered or may have suffered damage and a perpetrator made or may have made a profit, either intentionally or unintentionally;*
- *Any unlawful, unethical, or unauthorized behavior related to the automated processing and transmission of data is called computer abuse.”⁴*

UN Congress on Prevention of Cyber Crime and Treatment of Offenders:⁵

The United Nations Congress on the Prevention of Cybercrime and the Treatment of Offenders has described cybercrime as falling into two categories:

- **Narrow sense:** cybercrime is a computer crime that encompasses any criminal activity directed by electronic operations and aimed at the protection of computer systems and the data they process.
- **Broader definition:** Cybercrime in a broader context refers to all computer-related crimes and encompasses any criminal activity carried out on, *“or in relation to, a computer system or network, including illegal possession and offering or sharing information through a computer system or network.”*

1.2 Nature of Cyber Crime:

“The term cyber comes from the term cybernetics, which refers to the science of communication and control over machines and people.” Cyberspace is a new horizon for knowledge and communication between humans all over the world that is regulated by machines. As a result, *“crimes committed in cyberspace”* must be viewed as such. In a broader context, computer crime refers to any crime committed on the Internet, such as *“hacking, terrorism, fraud, gambling, cyber stalking, cyber theft, cyber pornography, virus transmission”*, and so on. Cybercrime encompasses both computer-related and computer-generated offenses. It is the source of global tension since it is growing at a rapid pace. As a result, law enforcement authorities must have a thorough understanding of the various types of cybercrime. Though the use of emerging technology by criminals is nothing new and in

⁴ S.T. Viswanathan, *The Indian Cyber Laws* 81 (Bharat Law House, 2001).

⁵ Tenth UN Congress on Prevention of Crime & Treatment of Offenders was held in Vienna on April 10-17, 2000.

this age of “*liberalization and globalization*”, we must acknowledge cybercrime as a major new phenomenon with global political, social, and economic implications. Cybercrime poses a challenge to the socioeconomic, political, and security systems of both the United States and other countries.⁶

1.3 Scope of Cybercrime:

Cybercrime is on the rise globally, not just in India. The amount of development made by a nation in information technology is directly proportional to the occurrence of cybercrime. According to a United Nations survey⁷, “*more than half of websites in the United States, Canada, and Europe have suffered security breaches and threats of cyber terrorism, posing a significant challenge to law enforcement agencies*”. In recent years, a new trend has emerged in which terrorists are heading for terror training. For militants who use the Internet to educate recruits in cyber terrorist training camps, it has become a primary teaching tool.

“Computer-related crime has already become a major source of concern in most countries around the world, and India is no exception”. The most important factor to consider when determining if a specific computer-related activity should be classified as cybercrime is the distinction that must be made between what is immoral and what is illegal. And when an action is actually unlawful should it be considered as a felony, and the perpetrator should be prosecuted. As a result, when deciding cases involving cyber law, criminal law should be applied with caution.

There has been a lot of controversy among legal experts about the terms "data misuse" and "computer harassment," which are often used in the sense of cybercrime, since there isn't a globally accepted concept of cybercrime or computer crime. “However, the current vogue in this regard is to believe that the two words have different meanings. The criminal law governing cybercrime must distinguish between accidental computer system misuse, reckless computer system misuse, and malicious computer system misuse, with the latter being classified as a crime rather than the former two. As a result of this distinction, it is the misuse of a computer device that should be considered as illegal activity punished by statute, not the behavior that causes the computer user inconvenience or discomfort.”

⁶ Douglas Thomas & Brian D. Loader, *Cybercrime: Security & Surveillance in the Information Age* 3 (1st ed., 2000).

⁷ U.N. Report on International Review of Criminal Policy and Prevention & Control of Computer Crime (Oct, 2005.)

1.4 Characteristics of Cybercrime:

The following are some of the most prominent characteristics of cybercrime:

Low-risk, high-reward ventures: *“Cybercrime is notable for being relatively easy to commit, difficult to detect, and much more difficult to prove. Cyber criminals with basic programming skills and experience can easily destroy valuable databases, causing significant financial loss or harm to the victims of the crime.”*⁸

Victims' lack of awareness: Many victims of cybercrime are unaware that it has occurred due to a lack of sufficient expertise and knowledge in operating a computer device.

No Physical presence required: Cybercrime can be perpetrated from afar without the need for the suspect to be physically present at the crime scene.

Lack of high-tech skills among law enforcement agencies: Detecting cybercrime necessitates high-tech skills, which most investigators lack.

Victims do not report incidents: In most cases, the group or company that has been victimized by cybercrime chooses not to report it to the police because they are afraid of negative attention or losing public confidence. The victims' unwillingness to come forward and file a police report adds to the seriousness of the cybercrime detection and control issue. There is no brutality involved. Cybercrime is not a violent crime; rather, it is the result of greed, malice, and manipulating the victim's vulnerability.

No territorial borders: The issue of cybercrime is exacerbated by the fact that the Internet has no territorial boundaries, allowing criminals to operate beyond the scope of the law in the vast majority of cases.

Privacy and Transparency: *“The computer network used for knowledge dissemination has anonymity and openness features that make it simple and convenient for the perpetrator to commit crime without being detected or recognized by the computer user who is a victim of his illegal behavior.”*

Lack of authentic evidence: Since all information over a network system is shared in the form of electronic data, there is no sign of data until it is deleted, and the suspect may remain undetected and avoid criminal investigation by destroying this sole evidence.

⁸ S.K. Bansal, Cyber Crime 17 (APH Publishing Corporation, 2011).

Have broader ramifications: The scope of cybercrime is wide enough to impact people's socioeconomic and legal rights.⁹

1.5 Elements of Cyber Crime:

With a few exceptions, there are two aspects of a crime: “Mens Rea and Actus Reus. For example, only mens rea is sufficient to impose criminal liability in conspiracy, while only Actus Reus is sufficient to impose criminal liability in crimes against the state such as falsifying evidence, counterfeiting coins, white collar crime, and so on. The basic principle of criminal law is that no one can be convicted of a crime unless the prosecutor can show beyond a reasonable doubt that his conduct (act or omission) is forbidden by criminal law and that he is responsible for it, as well as that he had a specific state of mind while committing the crime. As a result, Actus Reus without mens rea is not a felony. Actus Reus, according to J.C. Smith and B. Hogan, is a product of human action that the statute aims to avoid. In the case of cybercrime, proving all aspects of the crime is extremely difficult.”¹⁰

Actus Reus: *“Cybercrime's Actus Reus is very complex and diverse. For example, when using a keyboard and mouse to operate a device, when attempting access to information on another's computer without the permission or approval of the approved individual, when attempting hacking, spreading viruses, or committing cybercrime and actually causing such actions, and so on. There are human actions or Actus Reus in cyberspace that the law tries to avoid, i.e. they are cybercrime Actus Reus.”*¹¹

Mens Rea: Another important aspect of cybercrime is mens rea. According to Smith and Hogan, until the 12th century, “a person could be held responsible for any injury only for Actus Reus, which required no evidence of mens rea or a blameworthy state of mind”. This definition has changed in modern Common Law, and now a guilty mind is required for the commission of a crime and the application of a punishment. The IPC does not use or describe the word "mens rea." Mens rea is represented by the use of terms like fraudulently, dishonestly, intentionally, recklessly, motive, and so on. For example, hackers who commit hacking have knowledge or intent of gaining unauthorized access and thus committing cybercrime.

⁹ Ashish Pandey, *Cyber Crimes: Detection & Prevention* 126 (JBA Publishers, 2006).

¹⁰ J.C. Smith & B. Hogan, *Criminal Law* 103 (Lexis Nexis UK, 2002).

¹¹ *Id.*

1.6 Factors Responsible for Cyber Crime:

Professor H.L.A. Hart explained in his classic book, *The Concept of Law* that human beings are vulnerable to criminal actions that are crimes, and that rules of law are necessary to protect them from such acts.¹² Applying the same comparison to cyberspace, computer systems are highly fragile, despite being high-tech computers. By gaining illegal or unauthorized entry, this technology can easily be used to dupe or hack an individual or his device. The victim may have suffered direct or indirect harm as a result of the misuse of computer systems. Since there is no foolproof system in place to defend and safeguard innocent computer users from cyber criminality, cyber criminals continue to engage in illegal activity across networks without fear of being caught and prosecuted for the crimes they committed.

Huge data storage capacity: The device has the unusual ability to store large amounts of data in a limited amount of space. In a CD-ROM, a small microprocessor computer chip can store lakhs of pages. This storage capacity provides enough space to more easily delete or derive information via physical or visual mediums. Even if the power is switched off, *“any data stored in ROM will remain intact. Regardless of the form of ROM used, the data stored therein is non-volatile and will remain so unless it is purposefully deleted or overwritten.”*

More and wider information is available: A computer is an electronic system that performs its functions using complex technology rather than manual actions performed by humans. In the computer era, the greatest benefit of networking is the increased access to information services over a vast and comprehensive medium. More and more businesses are turning to networks to provide easily accessible information to their employees, clients, and other business partners. This is why; in today's information age, networking and cyber activities are becoming increasingly popular. The World Wide Web's sharing of information has provided new tools for easier and quicker access to information around the world. It has given rise to a new world of e-mails, chats, and downloads, among other things. *“Everyone is now just a mouse click away from everyone else. However, greater access to information causes some issues, such as securing and defending every data device against unauthorized*

¹² H.L.A. Hart, *The Concept of Law* 73 (Oxford University Press, 3rd ed., 2014).

access where there is a risk of violation, not due to human error, but due to complex technical manipulations."¹³

Computer systems' complexity: Machines run on operating systems, which are made up of millions of lines of code. "The human mind is fallible, and it is likely that a lapse could occur at any time. Cyber criminals take advantage of these flaws and vulnerabilities to gain access to the operating system. Hackers are cybercriminals who take advantage of flaws in current operating systems and security equipment. As a result, hackers are the feared enemy of the Internet and general network security, and they take advantage of the complexity of computer systems for personal gain, sabotage, fraud, greed, or malice towards the victim."

Negligence on the part of network users: Negligence is linked to human behavior. As a result, it is highly likely that when securing the computer system, the user may make a mistake or be negligent, allowing a cybercriminal to obtain unauthorized or unlawful access to or control over the machines. Interaction with a diverse group of computer users has shown that, in their haste to get the computer program up and running, they overlook access, control, and security controls, allowing cyber criminals to intrude and steal, change, or delete significant data. This is especially true for large organizations such as banks, companies, government departments, and others that have high-tech software systems for public access but leave them completely unsecure and unguarded against information poachers or manipulators due to gross negligence on the part of their staff or employees.¹⁴

Non-availability or lack of evidence: Digital data processing and network technologies have replaced conventional methods for generating, storing, distributing, and disseminating information or documents. The real problem facing law enforcement and investigation agencies is obtaining and preserving facts. Unlike conventional crimes, gathering adequate evidence of a cybercrime that can withstand judicial review to prove the cyber accused's guilt beyond a reasonable doubt is extremely difficult.

The anonymity provided by the Internet allows cyber criminals to engage in illegal activity without leaving any evidence, and even if evidence is left, it is not enough to persuade the police that a criminal case can be filed against the perpetrator. The low rate of

¹³ *Supra* note 12.

¹⁴ James R. Richards, *Transnational Criminal Organizations, Cybercrime and Money Laundering* 87 (Routledge, 1998).

cyber convictions indicates that most cyber criminals delete evidence in order to avoid being prosecuted. Due to the inadequacy of conventional methods of evidence and crime detection, cyber forensics has become a modern techno-legal practice. Although forensic experts play an important role in gathering and presenting admissible electronic evidence, as well as searching for and seizing material evidence related to the cybercrime under investigation, there are still some gray areas that enable the cybercriminal to tamper with the evidence and deceive the investigative agencies.

1.7 Classification of Cyber Crime:

A. Based on Old or New Computer-Related Crimes:

- **Internet-based crimes:** *“There are old crimes that are perpetrated on or by the internet's new medium. For example, on or by or with the aid of the internet, stealing, theft, misappropriation, slander, attacks, and so on. With its speed and global reach, the internet has made these crimes even more convenient, efficient, risk-free, inexpensive, and profitable to commit.”*
- **Internet-related crimes:** There are modern crimes that have arisen as a result of the internet, such as hacking, virus distribution, and intellectual property theft.
- **The use of new offences to commit old crimes:** For example, where cyber fraud is perpetrated by hacking.

B. Based on the Victim of Cyber Crimes:

Cybercrime can be narrowly categorized under the following three headings, depending on the victim:

- **Individuals:** It can be used against persons or individual property within this category by using the following methods:
 - *“Harassment via e-mail;*
 - *Cyber stalking;*
 - *Dissemination of obscene material;*
 - *Defamation;*
 - *Unauthorized control/access over computer system;*
 - *Indecent exposure;*

- *E-mail spoofing;*
 - *Cheating and fraud;*
 - *Computer vandalism;*
 - *Transmitting virus;*
 - *Net trespass;*
 - *Intellectual property crimes;*
 - *Internet time thefts.”*
- **Organizations:** Cybercrime against organizations may take the form of:
 - *“Unauthorized control/access over computer system;*
 - *Possession of unauthorized information;*
 - *Cyber terrorism against government organization;*
 - *Distribution of pirated software etc.”*
- **Society:**
 - *“Pornography;*
 - *Indecent exposure;*
 - *Trafficking;*
 - *Financial crimes;*
 - *Sale of illegal articles;*
 - *Online gambling;*
 - *Forgery.”*

C. Based on the Computer's Role:

The computer may be involved as a victim of crime, an instrument used to commit a crime, or a repository of evidence relevant to the crime, depending on the part played by the computer in the crime, as discussed under the following three headings:

Computer as the Victim: A machine or a computer network could be the object of an offense of which the computer is the perpetrator. The computer's confidentiality, honesty, or usability is jeopardized in such situations. The victim's information or service is compromised, or the victim is rendered disabled and injured.

Disrupting the operation of a device, computer system, or computer network; corrupting operating systems and programs; stealing or disrupting data or knowledge; intellectual property violations; and extortion using personal information hacked from computer systems are all examples of such crimes. Denial of service attacks on prominent internet sites such as Google, CNN, and the spread of the Melissa and I Love You viruses and their variants are examples of this type of computer crime.

Computer as the Tool: Frauds, IPR breaches, online sales of illicit products, and other crimes may all be committed using a computer as a tool or an active weapon. Computers may be used in the same way as any other high-tech device to commit conventional crimes. *“Frauds involving automated teller machines (ATMs), credit cards, electronic fund transfer (EFT) frauds, embezzlement of funds from banks, telecommunication frauds, counterfeiting, and software piracy are examples of such crimes. These types of crimes are also known as computer-assisted crimes. When a computer is used as an offensive tool in the commission of a crime, it is referred to as digital crime, since it could not be carried out without the use of information technology.”*

Computer as the Witness: A machine can be more than just a victim or a tool; it can also be a witness to the crime. Money laundering, illicit financial transfers, bulletin board systems (BBS), and the storage of drug distribution transaction documents are all examples of computers as witnesses to crime (viz. the purulia arms drop case, wherein the details of money transactions were stored in a laptop computer). A computer system can also be used to identify information that aids the suspect in committing the crime. For example, in the United States, an employee of Barclays Bank used the bank's computer to find a dormant account, forged the account holder's signature, and withdrawn \$ 2,100. In such instances, the machine is merely a byproduct of other crimes.

D. Bases on the Criminal Activities:

Physical Crimes: These crimes are those that include a device or its associated peripherals, hardware, software, or computer time. Robbery, breakage, data, performance, or media destruction, and inter-processing manipulations are some examples.

Data - Related Crimes: In data-related crimes, offenders insert illegal data or information in digital form into computer networks, or they modify, suppress, or manipulate data that should be entered in order to achieve an unfair advantage. The most popular form of

computer crime is input manipulation, which is both easy to commit and difficult to detect. The following four categories may be used to classify data-related crimes:

- **Data tampering:** This is the most common form of computer crime, involving input manipulations. It entails altering data with malicious intent during or before feeding it into a device in order to give a particular party an unfair advantage. It also involves inserting false input data, modifying the input data, omitting the desired input data, posting a transaction incorrectly, making changes or modifications to the master file records, partially posting transactions, deleting the output, and substituting the counterfeit output. Anyone involved in the process of making, capturing, encoding, analyzing, testing, converting, and transporting data that enters a computer may cause such changes.
- **Data leakage:** This refers to the unauthorized copying of a computer's master file information *“for ransom, extortion, or other fraudulent purposes.”*
- **Data eavesdropping:** To eavesdrop on a person's private details, his computer network is assessed from a remote location using a legal password or by cracking the password. Such information is sold for a very high price to others.
- **Scavenging:** This is a way of extracting or reusing information that has been left in or near a computer device after processing.

Crimes Involving Software: The device as well as the application software are affected or manipulated in such crimes. It is difficult to identify since this is a highly advanced and dangerous type of crime. It often entails modifying or adding new programs or procedures into the operating system, with computer programmers, researchers, and other specialists involved in commissioning or making changes to the software. Computer bugs, computer worms, Trojan horses, trap doors, super zapping, wire-trapping, time bombs, logic bombs, and salami attacks, among other tactics, may be used to commit software-related crimes.

CHAPTER 2

EMERGING CHALLENGES OF CYBER CRIME & SECURITY

2.1 Introduction:

To combat cybercrime in India, the Information Technology Act was passed in 2000 and then revised in 2008. However, due to the rapid growth of Internet technology, even after 17 years, there are several challenges. It's also due to an increasing reliance on the internet for e-commerce and other services. Attacks on critical infrastructure are becoming more pervasive, and risks to critical infrastructure are on the rise (WannaCry, Petya like mass cyber-attacks) Industrial systems are vulnerable because they are not smart computers, but rather devices such as SCADA and other industrial automation products that lack a security definition. With the popularity of Blue Whale and an increase in questionable applications and websites that promote the challenge, threats to children are on the rise. Fraudulent job offers are on the rise: Fraudsters are stealing small sums of money from students, ranging from \$1,000 to \$20,000, under the guise of providing them with a job or an internship. In most cases, money is requested to be sent through PayTm or other mobile wallets. The numbers are then turned off or, in some cases, turned on, and rackets are set up, but there is underreporting and the quantities are so small that police are often hesitant to investigate. Financial cybercrime is also on the rise: Crimes involving the vishing process of requesting an OTP are active. The states of West Bengal, Jharkhand, and Chhattisgarh are responsible for the majority of the attacks. All of the callers are involved and appear to be outside the control of any law enforcement agency, so they don't mind if things are recorded.¹⁵

During the last year, India has experienced a series of major and unprecedented events that have taken the question of cyber security for the Indian banking sector to the forefront like never before.

The ongoing initiative of the Government of India, through its flagship Digital India programme, with a vision to turn India into a digitally empowered society and information economy has been the most significant factor in this regard. The rapid increase in the value and volume of digital transactions, which reached new highs in March 2017, demonstrates

¹⁵ Ahmad Tabrez, Challenges of Cyber Crimes in India: A Critical Analysis (May 12, 2018). 22nd World Multiconference on Systemic, Cybernetics and Informatics (WMSCI 2018) by International Institute of Informatics and Systemic, Orlando, Florida, USA, July 8-11, 2018, Available at SSRN: <https://ssrn.com/abstract=3177396>.

the rapid shift to electronic payments. With the total number of accounts reaching 42.31 crore¹⁶, the Pradhan Mantri Jan Dhan Yojana (PMJDY) has continued to increase the penetration of inclusive banking, bringing the uninitiated and new users into the fold of banking services. Risk concerns and events made their presence known as well. The compromise of a major bank's SWIFT payment application and subsequent large-value fraudulent fund transfer¹⁷ and the large-scale compromise of multiple banks debit cards by an advanced and persistent assault on a payment processor¹⁸ were two of the major events. These incidents have raised the bar on the severity of cyber-attacks to new heights. India is on its way to become a digital economy, thanks to digitization. For the vast Indian population, digitization provides unrivaled functionality, coverage, and usability. When a resource becomes central to competition but insignificant to strategy, as Nicholas Carr famously said, the threats it causes become more valuable than the advantages it provides. If the benefits of digitization are to be reaped and spread to Indian people, cyber risk now ranks among the existential risks for Indian banks, and it is critical that policy makers regard it as such. In India, the digitization of financial transactions is picking up speed. Noncash payment transactions, which currently account for 22% of all customer purchases, are expected to surpass cash transactions by 2023.¹⁹ By 2020, total payments made using digital payment instruments are expected to be in the amount of USD 500 billion, which are roughly ten times current levels. With 100 crore mobile connections in the world, 24 crore of whom are smartphone users, the country's technological infrastructure continues to develop. By 2020, the number of smartphones will have risen to 52 crore. Around 90% of all devices have internet access, and internet users are expected to double to nearly 650 million by 2020, up from 300 million in 2015.

Meanwhile, Aadhaar enrolments are nearing saturation, with two states already reporting 100 percent coverage.²⁰ This has major consequences for KYC simplification, as well as the spread of services like the “*Aadhaar Enabled Payment System (AEPS)*.”

¹⁶ *Progress Report*, Pradhan Mantri Jan Dhan Yojana (Apr 28, 2021), <https://www.pmjdy.gov.in/account>.

¹⁷ *The Making of a \$500 Billion Ecosystem in India*, The Boston Consulting Group (Jul, 2016), https://image-src.bcg.com/BCG_COM/BCG-Google%20Digital%20Payments%202020-July%202016_tcm21-39245.pdf.

¹⁸ Suresh Krishanmoorthy, *Telangana is No. 2 in 100% Aadhar Enrolment*, The Hindu, July 19, 2017.

¹⁹ Amber Sinha & Srinivas Kodali, *A Documentation of public availability of Aadhar Numbers with sensitive personal financial information*, The centre for internet & society (May 1, 2017), <https://cis-india.org/internet-governance/information-security-practices-of-aadhaar-or-lack-thereof-a-documentation-of-public-availability-of-aadhaar-numbers-with-sensitive-personal-financial-information-1>.

²⁰ Surabhi Agarwal, *E-Authentication a must to curb Aadhar frauds*, ET, July 26, 2017.

As previously stated, the PMJDY accounts widened the reach of financial inclusion, with nearly 18 crore accounts in semi-urban and rural areas. It's important to remember that the majority of these account holders would be unfamiliar with banking processes and the technology infrastructure that supports them, rendering them vulnerable to social engineering and other cyber-attacks. Indian FinTech firms, which are growing in number and complexity, have played a key role in the exciting growth of the payment ecosystem. These businesses would most likely use technology to connect with banks and the Aadhaar database. Payment networks, peer-to-peer and cross-border transactions, as well as mobile point-of-sale processing, are among the active areas; robot-advisory and brokerage for personal finance management; crowd-funding, P2P lending, alternative lenders, and market places; and credit scoring, analytics, and risk management are among the active areas.

These latest applications are expected to add complexity to system interfaces, potentially exposing cyber vulnerabilities and data protection concerns. Furthermore, as FinTech companies begin to differentiate themselves based on data, data privacy and consumer security will become more relevant. FinTech firms may have access to confidential financial details about consumers, but they will also likely gather personal information about them in their search to learn more about them. In the event of a cyber-attack, interfaces and APIs that allow for smooth data transfers between multiple applications can be the most vulnerable and provide opportunities for malware propagation. Developing good defense mechanisms and procedures to resolve these issues, just as it is for *“incumbent banks and financial institutions, will be critical for the FinTech market.”*

People are gradually disclosing personal information to the general public. Government and private sector actors now have access to an unparalleled amount of personal data. *“Digital India, Aadhaar, and telecom initiatives have contributed to the already large pool of personal data used by various public and private entities to carry out their operations.”* Due to a lack of awareness of the security and privacy consequences, a vast volume of data could have already been exposed.²¹

Since the majority of Indians are *“digital immigrants and therefore vulnerable to data misuse”*, publicly accessible personal sensitive information may pose a danger to them. Individuals often share and transmit personal information for a variety of purposes.

²¹ Sugata Ghosh & Sangita Mehta, *Pakistani hacker defaced Canara Bank site, tried to block e-payments*, ET, Aug 11, 2016.

Individuals do not know the reason for gathering personal information, how that information will be used, the protection protocols in place to protect that information, how long that information will be kept, and how that information will be destroyed, *“nor have these aspects been specified universally in policies and procedures. India does not have any clear data security regulations.”*

2.2 Major Types of Cyber Crime in India:

Hacking: A hacker is an unauthorized person who tries to gain access to a computer system or succeeds in doing so. Since it is an assault on data protection, hacking is a crime even though there is no apparent harm to the device.

Cyberstalking: This crime entails harassing others via the internet. False allegations, intimidation, and other forms of behavior are examples. Typically, men are the majority of cyber stalkers, while women are the majority of victims.

Spamming: It is the practice of sending unsolicited commercial and bulk messages over the internet. While most email users find it annoying, it is not illegal unless it causes harm to the network, disrupts service to customers, or makes. Consumer perceptions of Internet Service Providers are negatively affected.

Cyber Pornography: On the internet, women and children are sexually exploited. Pedophiles use the internet to submit images of illicit child pornography to specific children in order to entice them to participate in such activities. They are later sexually abused for profit.

Phishing: Phishing is a criminally deceptive method of obtaining personal information such as usernames, passwords, and credit card numbers by impersonating a reliable entity in an electronic message.

Software Piracy: It is the unlicensed copying and distribution of software for commercial or personal purposes. This is considered a copy right infringement as well as a license agreement violation. It is impossible to find solutions since the unauthorized user is not a party to the license agreement.

Corporate Espionage: This refers to the stealing of trade secrets using unlawful methods such as wiretaps or illegal intrusions.

Money Laundering: This refers to the movement of illegally obtained funds through financial and other processes in order for them to appear to have been obtained lawfully. For example, transport cash to a country with laxer banking regulations and then return it via loans, the interest of which can be deducted from his taxes. Prior to computer and internet technology, this was possible; however, electronic transactions have made it simpler and more effective.

Password Sniffers: Password sniffers are programs that track and record network users' names and passwords as they log in, jeopardizing site security. Anyone who installs the sniffer has the ability to log in as an approved user and gain access to restricted documents.

Spoofing: This is the act of making one device appear to be another computer electronically in order to obtain access to a system that is usually limited.

Web Jacking: This phrase refers to the unauthorized access to a website by breaking the password.

Cyber Terrorism: Cyber terrorism is the use of computer resources to threaten or coerce the government, the civilian population, or any part thereof in order to achieve political or social goals. Individuals and organizations often attempt to use the internet's anonymity to intimidate governments and terrorize the country's people.

E-Mail Bombing: This is a serious crime in which an individual sends a large number of emails to the target system's or person's inbox. Mail bombs usually occupy the allotted space on an e-mail server for the users' e-mail, causing the server to crash.

Computer Virus Spread: A computer virus is a series of instructions capable of performing malicious operations. Viruses disrupt the regular operation of machine programs and, in some cases, the whole operating system. They can also wreak havoc on your machine, rendering it unusable until the operating system is reinstalled. Emails, CDs, Pen drives (secondary storage), Multimedia, and the Internet can all be used to spread computer viruses.

Online Fraud: Online fraud may take place in chat rooms, email, message boards, and websites. In cases such as online shopping, real estate, pay BAL, and work-at-home donation processing, an internet fraudster may submit false information to the victim.

Cyber Warfare: It is a form of Internet-based conflict that involves politically motivated attacks on computer systems. Cyber warfare attacks can cripple financial systems,

interrupt or disable essential services, steal or modify sensitive data, and disable official websites and networks, among other things.

SMS Spoofing: SMS Spoofing enables you to change the name or phone number from which text messages are sent.

Speech Phishing: It is a phrase that combines the words "voice" and "phishing." Voice phishing is a method of gaining public access to private, personal, and financial information. To obtain details, voice phishing uses a landline phone call.

2.3 Impact of Cyber Crime:

Impact on the Economy: For money transfers and payments, people today rely heavily on computers and the internet. As a result, the likelihood of becoming a victim of online money fraud is extremely high. With the rise in popularity of "cashless India" in India, the chances of being duped online are also rising, if one is not careful enough to use secure online transaction platforms and applications.

Not only individuals experience financial losses as a result of cybercrime; according to some studies, approximately 80% of businesses involved in the surveys admitted financial losses as a result of cybercrime.

Personal Information Leakage: People experience not only financial losses, but also personal information leakage. Even if a social networking site is safe, it is also an open forum for everyone to see another person's life, which can be risky. Aside from that, hackers can break into a user's account and steal any information they want. People are also harmed by spam and phishing.

Loss of Consumer Trust: As a result of such financial losses and the risk of personal information being compromised, customers begin to lose confidence in such websites and apps. Even if the crime is committed by someone else, the platform or app is flagged as fraudulent and dangerous. People are also hesitant to begin a transaction when their credit card information is requested. This damages e-reputation businesses and, as a result, jeopardizes a future business.

The Challenge to National Security: Most countries' militaries now employ sophisticated computer technology and networks. Information warfare, while not new, is still used to spread malware that can cause network outages and spread false information.

Terrorists and cybercriminals, in addition to militaries, use these tools to break into other countries' security networks and steal information. They often use computer systems to transmit threats and alerts.

2.4 Major Challenges:

Incidents & Threats:

According to PwC's Global Economic Crime Survey²², cybercrime has risen to second place as the most commonly identified economic crime, with financial institutions being prime targets. Threat trends including phishing, spear-phishing, and social engineering grow and become more advanced as cybercriminals discover new ways to strike, hack, and manipulate organizations. Organizations include real-time vulnerability assessments of both their own and their vendor's vulnerabilities. Banks in India have been targeted by potential state and non-state actors, organized crime, and hacktivists on a regular basis. This was demonstrated in the case of Canara Bank, which was targeted and defaced by a hacker from Pakistan in August 2016, who inserted a malicious website and attempted to block some of the bank's e-payments. In July 2016, the Union Bank of India was also the target of an attack. Cyber robbers came close to stealing USD 171 million from the company's Nostro account. Using spoofed RBI IDs, the attackers allegedly obtained access via spear-phishing. Unfortunately, one of the officials was duped by the phishing email and clicked on the malicious connection, allowing malware to infect the computer. The attempted cyber theft of USD 81 million from the Bangladesh central bank's account at the New York Federal Reserve was strikingly similar. The Union Bank data breach highlighted a few key points for financial and banking institutions. The first is the ever-changing existence of new malware; the second is the value of organizational security awareness; and the third is the efficacy of current security management activities. There was no loss to the organization due to effective action on the part of Union Bank of India, illustrating the value of incident response readiness. A new way to assault a bank has been published from Brazil. On a weekend afternoon in October 2016, a bank's DNS records were changed to point to fake pages, redirecting legitimate traffic to 36 of the bank's web assets and potentially exposing customer credentials. It's possible that ATM and Point-of-Sale networks were also hacked. Customers

²² Steve Morgan, *Cybersecurity Spending outlook: \$1 trillion from 2017 to 2021*, CSO (June 15, 2016), <https://www.csoonline.com/article/3083798/cybersecurity-spending-outlook-1-trillion-from-2017-to-2021.html>.

were exposed to more harm by fake sites that included malware in the form of a Trustee update. Some of the global trends mentioned below have implications for Indian businesses:

- **From 2017 to 2021, cybersecurity spending is projected to reach \$1 trillion.** According to Gartner, the increase in cybercrime has driven spending on goods and services to more than \$80 billion in 2016. Researchers and IT analyst firms are finding it difficult to reliably predict spending due to the rise in cybercrime. Over the next five years²³, from 2017 to 2021, global spending on cybersecurity products and services is expected to reach \$1 trillion.
- *“Frost & Sullivan predicted a 1.5 million labor shortage by 2020 in 2015. The prediction has been updated to a 1.8 million worker shortage by 2022”*, based on recent events and shifting market dynamics. Unfilled cyber security vacancies are expected to hit 3.5 million by 2021, according to a study by Cyber Security Ventures.
- Microsoft predicts that by 2020, 4 billion people will be online, more than double the current figure. Humans have surpassed computers as the top priority for cyber criminals as the world becomes more interactive.

Systematic Challenges:

The following are some of the factors that continue to have an effect on the state of cyber security:²⁴

Internal employee awareness remains low: Internal employee awareness remains the first line of defense. However, few businesses invest in cyber security awareness training and improvement.

Inadequate budgets and a lack of top-level support: Budgets are typically dictated by business needs, and cyber security is given a low priority. Support for cyber security initiatives is typically given low priority by top management, which is another source of concern. This is largely due to a lack of understanding of the risks' consequences.

Identity and Access Management (IAM) Issues: *“Identity and access management is a critical component of cyber security. In an age where hackers seem to have the upper*

²³ Steve Morgan, *The human attack surface, continuing it all up*, CSO (Dec 12, 2016), <https://www.csoonline.com/article/3149510/the-human-attack-surface-counting-it-all-up.html>.

²⁴ Nandkumar Saravade & Ambuja Bhalla, *Emerging trends and challenges in cyber security*, REBIT, <https://rebit.org.in/whitepaper/emerging-trends-and-challenges-cyber-security>.

hand, all it takes is one corrupted password to gain access to a corporate network. Despite some progress, much more work needs to be done in this sector.”

Ransomware is on the Rise: Recent malware attacks, such as WannaCry and Petya, have highlighted the growing threat of ransomware. Criminals are looking at other vectors as more users become aware of the risks of ransomware attacks via email. Some are experimenting with malware that re-infects after a ransom is charged, while others are relying on built-in tools rather than executable malware to escape detection by endpoint security software that looks for executable files. Writers of ransomware are increasingly using methods other than encryption, such as removing or corrupting file headers.

Smart devices and apps: As more businesses embrace mobile devices as their primary mode of communication, hackers can increasingly target them. Since mobile apps can be used to conduct financial transactions, the mobile phone has become a more appealing target, resulting in a rise in mobile malware. The possibility of jailbroken and rooted devices being used for financial gain expands the attack surface.

DDoS attack: *“With the introduction of IoT-powered botnets, destructive DDoS attacks are unavoidable, and their volume and frequency have increased. To mitigate DDoS threats, Indian organizations must enhance their response capability.”*

Social Networking: As the use of social media grows, hackers will have more opportunities to manipulate it. Many users publish their information for everyone to see, which could be used to target the user's business. The use of social media to spread fake news may have a subtle effect on bank reputations.

2.5 Finding Solutions:

Many businesses and financial institutions are also vulnerable to a variety of material threats. They would be able to properly handle risks if they take the following strategy:²⁵

Integrated protection vs. layered defense: Since the financial services industry is heavily regulated, banks invest time, resources, and effort in implementing best-in-class technology, which, sadly, also runs in silos and is difficult to manage. It is critical to move toward integrated security, in which all components interact and collaborate.

²⁵ Nandkumar, *supra* note 21.

Prioritize risk-based security: Risks are ever-changing, and complete avoidance is impossible. A risk-based strategy provides a straightforward path for the company to concentrate its efforts and resources where they are needed most. It's a good idea to categorize the “risk associated with each method and target the efforts accordingly”.

Machine learning and big data analytics will help you become smarter and more intuitive: Given the current digitization push, the amount of data applicable to the BFSI sector will grow at an exponential rate. Analytics is one of the most important aspects of exploiting cyber resilience. *“A new breed of security analytics solutions has emerged, capable of storing and analyzing massive quantities of security data in real time.”*

Shift your mindset from protection as an expense to security as a benefit: The attitude of seeing protection as an expense must be changed. Organizations should see the advantages of proactive protection because of the *“dangers associated with security threats and the potential effects on business.”*

Investing in Next-Generation Endpoint Protection: Signature-based solutions are no longer sufficient and are vulnerable to zero-day attacks. Banks and other financial institutions must invest in technology that can detect and deter exploitative practices and behavior.

Basic Automation: Automation will free up resources for hunting, constructive security, and other activities by eliminating time spent on smaller, repeatable incidents.

Protect data: The standard solution has been to protect the data-holding structures. With data available in various formats (structured and unstructured) and stored on multiple devices and in the cloud, a paradigm shift is needed. It is recommended that, in addition to maintaining systems safe, information/data be protected such that protection is maintained and moves with it at all times.

Capabilities to React and Recover: It is not a matter of whether, but when, an organisation will be targeted. Organizations must be prepared to recognize and react to such attacks, as well as recover with minimal damage.

Denial & Deception: Deception tactics are commonly and efficiently used to improve threat identification and as a threat response tactic in strategic denial and deception. *“Deception technology is a promising new way to detect cyber-attacks that are undetectable.”*

It provides the company with a series of automated tripwires that can be used to turn the tables on even the most sophisticated hackers.”

2.6 ReBIT Initiatives:

The Reserve Bank of India (RBI) has formed Reserve Bank Information Technology Pvt. Ltd (ReBIT) to handle the bank's IT needs, including cyber security.²⁶

The Reserve Bank of Australia and its controlled entities ReBIT will concentrate on financial sector IT and cyber security (including related research) and assist in IT systems audit and assessment of RBI controlled entities; advise, execute, and manage Reserve Bank internal and system-wide IT projects (both existing and new) as mutually agreed upon by the Reserve Bank and ReBIT.²⁷ ReBIT will serve as a catalyst for creativity, large systems, and new concepts, as well as guiding controlled entities in IT-related areas of their operations and the RBI's IT-related functions and initiatives. ReBIT will effectively engage in the establishment of standards to enhance the Reserve Bank's position as regulator, given the need for interoperability and cross-institutional cooperation. ReBIT's objective will be supported by the following four verticals:

- I. Cyber Security:** For assurance and stability, improve the confidence and reliability of RBI's infrastructure through cyber security;
- II. Research and Innovation:** To strengthen the Indian banking industry by developing innovative technology solutions based on research and leveraging synergies among key stakeholders;
- III. System Audit:** Via excellence in audit, analytics, and forensics, support validation and implementation of regulatory guidelines on cyber protection for the banking sector;
- IV. Project Management:** To use lean and agile development capabilities to construct and operate dependable and motivating processes, as well as to have a delightful user interface.

Community Leadership: ReBIT's strategy is to collaborate with experts and push industry-led efforts to improve the financial sector's cybersecurity resilience.²⁸

²⁶ Nandkumar, *supra* note 21.

²⁷ *Id.*

²⁸ Nandkumar, *supra* note 21.

- **Working Group for the Cybersecurity Maturity Model:** ReBIT has collaborated with the banking CISO community to develop the maturity model. The working group is developing a Cybersecurity Maturity Model that can be used by financial institutions, financial software and other suppliers, security service providers, and other stakeholders to measure a firm's preparedness using consistent metrics;
- **Working Group on Cybersecurity Evaluation Framework:** This working group will draft specifications and an assessment model to improve the industry's overall cybersecurity posture. In an industry-led effort, the working group will define a cybersecurity evaluation model for financial firms. This will bring consistency to the audit process of controlled agencies, help clarify the nature of risk evaluations exercises with the appropriate regulatory supervision, and increase overall assessment effectiveness through a well-defined process that includes remediation monitoring and closure. In the long run, standards creation, process definitions, and regulatory tool sophistication would help bring automation, performance, and benchmarking to the industry, which would be extremely beneficial.

Operational Excellence: The Operational Excellence Initiative at ReBIT aims to develop cutting-edge capability. It currently includes a series of webinars on a variety of topics that will assist security professionals in the financial industry by exchanging knowledge on best practices, tools and technology for implementing these best practices, and case studies. The webinars will be registered and made available on the ReBIT website. In addition to the webinars, certain programs may need additional funding in order for financial institutions to easily implement these best practices. We're working on playbooks right now, with an emphasis on collaboration and advisory groups to help financial institutions adopt these best practices. The following topics have been discussed and presentation materials and playbooks have been made available on the ReBIT webinar repository.

Business Leaders' Forum: To promote and raise consciousness about cybersecurity initiatives.

- Campaign to Increase Cybersecurity Awareness
- **Periodic Cybersecurity Newsletters:** *“The target audience will include key RBI stakeholders (CGM and above), as well as CIOs, Executive Directors, business unit heads, heads of internal audit, operational risk, enforcement, and fraud management from all RBI-regulated financial institutions. Readership is targeted at the highest*

levels of management, who would be interested in the latest news and will be able to affect the latest thought and action on cybersecurity policy within their organizations.”²⁹

2.7 CERT – Fin on the Horizon:

The Indian government has announced plans to establish a Computer Emergency Response Team for the Financial Sector (CERT-Fin). The Ministry of Finance established a working group to collaborate closely on cyber security issues with all financial-sector regulators and stakeholders. The report of the working group was made public by the Ministry of Finance, which invited public consultation.

“CERT-Fin will compile, evaluate, and disseminate information on cyber incidents in the financial sectors, according to the WG report.” It will forecast cyber security incidents and submit warnings. It will also take immediate action in the event of a cyber security incident. It will coordinate cyber incident responses and operations, as well as issue vulnerability and information security recommendations, advisories, and white papers.

“CERT-Fin will monitor financial sector efforts to preserve modern cyber security infrastructure and raise awareness among controlled entities and the general public. It will also raise security awareness by disseminating information on its website and running a 24-hour incident response support desk. It will also provide incident prevention and response services, as well as quality management services, and perform functions similar to those performed by CERT-Fin”, which is responsible for priority cyber protection in the financial sector on a national level. All stakeholders, including regulators and the government, will receive policy recommendations from CERT-Fin to improve financial sector cyber security.

CERT-Fin is expected to make a major contribution to strengthening the Indian Financial Sector's cyber resilience.³⁰

There is no question that the complexities of protecting consumers' and citizens' knowledge and financial assets, as well as providing cutting-edge services in a dynamic market climate, would put financial institutions to the test. This is a multi-front war that requires meticulous planning, complete commitment, vigorous exercise, and flawless

²⁹ Nandkumar, *supra* note 21.

³⁰ Nandkumar, *supra* note 21.

execution. A collaborative approach can accomplish a lot while lowering business costs without sacrificing efficiency, confidence, or reliability.

CHAPTER 3

CYBERCRIME LEGAL CONTROL & REGULATION

3.1 Introduction:

The creation of law can be traced back to the beginnings of civil society. People began to live and work together as society progressed, forming groups that ultimately contributed to the establishment of the state. There was a need to regulate individual conduct; as a result, the state created the rules of government that later became known as law. As a result, legal growth is a continuous process that evolves in tandem with improvements and advancements in social circumstances. Law is usually created to meet the needs of society, and as a result, it is a complex principle that evolves as the needs of society change. Modern technological advancement has allowed human society to flourish and progress, but it has also given rise to new problems that were previously unknown to humanity, such as cybercrime, which arose just a few decades ago. People can now use the internet to visually talk, send messages, exchange information, and conduct business with people in every part of the world thanks to enormous advances in computer technology during the last quarter of the twentieth century. As a revolutionary mechanism, the machine has expanded our capacity to store, scan, retrieve, and communicate data, as well as our access to information, allowing us to communicate with everyone, anywhere, at any time.

The E-Commerce Act, 1998, established the legal structure for the cyber environment in India. Following this, there was a need for a simple legislation that covered all aspects of the cyber environment, so in May of 2000, India's Parliament passed the Information Technology Act, 2000, with the aim of combating cybercrime and providing a legal structure for e-commerce transactions. This was India's first cyber law, which dealt primarily with cybercrime. It covers a wide range of offenses committed in an electronic format or involving computers, computer systems, and computer networks. The Indian Penal Code, 1860; the Indian Evidence Act, 1872; the Bankers Book Evidence Act, 1891; and the Reserve Bank of India Act, 1934 are all amended by this Act. The Information Technology Act of 2000 (IT Act) has proven to be a divisive piece of legislation. The Act has gotten a lot of flak from the legal profession and the general public in its sixteen years of existence. It is said to have a slew of weaknesses, limitations, and pitfalls, ranging from ineffectiveness in combating cybercrime to unjust restrictions on citizens civil liberties. The Information Technology Act has been in effect in India since 2000 to combat cybercrime, but the issue is that it is still

more on paper than in practice because lawyers, police officers, prosecutors, and judges are unable to comprehend its highly technical terminology. It was implemented as India's basic law for cyberspace transactions, but due to certain flaws, it was revised in 2008 with the addition and replacement of new sections and sub clauses, among other things.

3.2 Need for Cyber Laws:

With the growing number of internet users, the need for cyber laws and their implementation has never been more pressing. Cyber laws are needed because of the following reasons:

With the rise in popularity of payment apps and sites, consumers are increasingly using online transactions because they are convenient and reliable. The government's "Cashless India" initiative has also gained traction, resulting in a surge in online transactions.

Email, SMS, messaging apps, and social media platforms have supplanted traditional communication methods.

To keep their electronic data secure, businesses rely heavily on their computer networks.

Most government forms, such as income tax returns, passport applications, Pan Card applications, and company law forms, are now filled out electronically.

Digital signatures and authorization are fast, and they can be used to replace traditional methods of transaction identification.

Computers and networks can also assist with non-cybercrimes. The majority of data is now stored on computers and cell phones. Kidnapping, terrorist attacks, counterfeit currency, tax evasion, and other crimes will all benefit from the evidence gathered from them.

Cyber laws aid in the representation and definition of the cyber society model, as well as the maintenance of cyber properties.

In today's world, digital contracts are becoming more popular; cyber laws help to protect the rights of these legally enforceable digital contracts.³¹

³¹ Diva Rai, *Cyber Crime and Cyber Law: An Overview*, IPleaders (Oct 15, 2019), https://blog.ipleaders.in/introduction-to-cyber-crime-and-cyber-law/#Need_of_Cyber_Law.

3.3 Conventions & Conferences:

To deter and fight cybercrime, many countries around the world have adopted their own criminal laws, computer laws, information technology laws, and intellectual property laws, among other things. However, because of the international nature of cybercrime, the issue of jurisdiction occurred more often when nationals or companies from two or more countries were involved in the crime, or when the criminal was of a foreign nationality and the crime was committed in a different country. The key issue, then, is determining which country's law should be used to settle the conflict or prosecute the criminal(s), particularly when different countries cyber and penal laws differ. The Internet, as a vast global network of computers, and the ability of cyber criminals to commit crimes from one location while remaining anonymous, necessitates the creation of a universal and uniform law governing and regulating cyberspace transactions in order to address the issue of cyber criminality by resolving the jurisdictional problem. The ever-increasing problem of cybercrime necessitates immediate concerted efforts on the part of all nations, governments, industries, technocrats, and jurists to develop uniformly unified legislation such that common offenders may be prosecuted and punished without legal or jurisdictional complications. The international community is making strenuous efforts in this direction to solve the issue of international cybercrime. Since internet operations are global in nature and do not acknowledge territorial or political boundaries, cyber criminals can operate across national borders without having to be physically present at the crime scene. As a result, greater international support and cooperation are needed to combat cybercrime. Though the United Nations has done a lot to encourage member countries to work together to combat cybercrime as a common cause, the response has not been very encouraging, except for the fact that there is a general consensus among countries that when a cybercrime involving a country or countries is involved, trans-border assistance and co-operation between the countries is necessary.

The 12th Conference of the Directors of Criminological Research Institutes of the Council of Europe, which addressed computer-related crimes for the first time in 1976, marked a turning point in global development in this direction. Following this meeting, the Council of Europe's Select Committee on Economic Crime undertook a review of economic crime in general and made recommendations on the subject. The Organization for European Co-operation and Development (OECD) began a study on the harmonization of international criminal laws in 1983, which culminated in the publication of the report Computer Related

Crime – Analysis of Legal Policy in 1986³². According to the study, countries should consider banning and penalizing a list of computer crimes by legislation and following points:

- *“The intentional input, modification, erasure, and/or suppression of computer data and/or computer programs with the intent of committing an unlawful transfer of funds or another valuable item;*
- *The intentional input, modification, erasure, and/or suppression of computer data and/or computer programs in order to commit a forgery;*
- *Input, deletion, erasure, and/or suppression of computer data and/or computer programs, as well as other computer system interference, done with the intent to obstruct the operation of a computer and/or telecommunication system;*
- *Infringement on the owner's exclusive right to a protected computer program with the intent to commercially manipulate and sell the program;*
- *Unauthorized access to or interception of a device and/or telecommunications system, either (i) due to a breach of security controls or (ii) for other misleading or malicious purposes.”*

Following that, the Council of Europe began its own investigation into computer crime with the aim of developing recommendations to assist policymakers in determining the extent and complexities of computer-related crime.³³ These proposals were adopted by the Council of Europe's Committee of Ministers in September 1989. Business transactions are now conducted over the internet, and online transactions have opened up new avenues for unscrupulous cyber criminals to defraud and cheat legitimate businessmen and consumers. In response to the growing threat of cybercrime, the United Nations Congress adopted a resolution in 1986 at its 13th Plenary Session, urging member states to step up their efforts to fight cybercrime through appropriate legal steps.

Since Internet operations are global in scope, they are not bound by any territorial boundaries. This allows cyber criminals to function outside of national geographic boundaries without having to be physically present at the crime scene. As a result, the issue of cybercrime necessitates greater international support and cooperation. Though the United Nations has done a lot to encourage member countries to work together to combat cybercrime

³² 87(2) OECD, *Computer Related Crime: Analysis of Legal Policy* (1986).

³³ S.T. Viswanathan, *The Indian Cyber Laws* 104 (Bharat Law House, 2001).

as a common cause, the response has not been very encouraging, except for the fact that there is a general awareness among countries that when a cybercrime involving a foreign country or countries is involved, trans-border assistance and cooperation between countries is needed.³⁴

International de droit Ponel Conference – Germany, 1992:

The colloquiums on Computer Crime and Other Crimes against Information Technology were held in Wartzburg by the Association International Droit Ponel (ADIP) (Germany). According to the survey, only 5% of computer crimes are reported to the police. According to the study, the following factors contribute to cybercrime non-disclosure:

- *“The operational speed and storage space of computer hardware make it extremely difficult to detect illegal activity;*
- *Law enforcement agencies lack the technical capabilities needed to combat cybercrime;*
- *Victims of these crimes are afraid to report the crime to the police because they fear being harassed and wasting time and resources in this futile endeavor;*
- *The victim is often afraid of negative attention if he or she reports the incident;*
- *Non-reporting of cybercrimes may be due to a variety of reasons, including a loss of goodwill, public confidence, investor faith, or embarrassment.”³⁵*

22nd G-7 Summit on Cyber Crime, 1996:

At the G-7 Summit on Terrorism in Leon (France) in July 1996, the member nations³⁶ agreed to speed up mutual consultations and cooperation on encryption by holding appropriate bilateral and multilateral meetings on encryption that allows lawful government access to data and communications in order to prevent or investigate acts of cyber terrorism while protecting the privacy of legitimate citizens. In light of the global existence of information and communication networks, the member countries have stressed the importance of encouraging non-member countries to accept the G-7 Summit's guidelines. The focus of the discussion was on information system security, personal data privacy, and the protection of people's intellectual property rights. To raise awareness of the threat of

³⁴ 66th U.N. General Assembly Annual Conference of the Interpol held in New Delhi in October, 1997.

³⁵ Kamshad Moshin, *Global Perspective of Cyber Crimes & Related Law* (2020), SSRN Electronic Journal. 10.2139/ssrn.3673938.

³⁶ The group of G-7 countries consisted of Canada, France, Germany, Italy, Japan, UK and USA.

cybercrime and encourage countries to address the issue on a global scale, efforts were made to provide required training through international law enforcement academies in Budapest, Hungary, Bangkok, Thailand, and other locations. Aside from that, the US National Infrastructure Protection Center hosted workshops with other countries to exchange knowledge on cyber intrusion prevention techniques.³⁷ In September 1999, a Cybercrime Conference was held in New Orleans to provide training to law enforcement officials from various countries.

G-8 High Tech Crime Working Group, 1998:

A G8 Hi-Tech Crime Sub-Group³⁸ was created in March 1998 as part of the international cooperation program to fight cybercrime, to provide trans-border access to stored data and assistance in hi-tech crime investigations involving the unauthorized modification or dissemination of electronic information. In 1998, a G-8 Sub-Group Conference in Paris (France) brought together members from industry and consumer groups to address issues relating to internet protection that affect industrial and consumer establishments, as well as how to create a safe and secure atmosphere for e-commerce.

Paris Cyber Crime Conference, 2000:

In May of 2000, a three-day Cybercrime Conference was held in Paris, attended by approximately 300 delegates from G-8 nations, including judges, police officials, ambassadors, legal experts, leading businessmen and industrialists. The conference emphasized the importance of enacting a global law to combat hackers, software pirates, crooks, and virus attackers who were making internet users lives miserable. The members unanimously agreed that an international conference to discuss cybercrime issues was required, as well as the importance of establishing an International Criminal Tribunal with global jurisdiction to deal with cybercrime and criminals. It was also decided that the existence of cybercrime necessitates active cooperation and coordination among the concerned countries in the investigation and prosecution of these high-tech crimes, regardless of territorial boundaries. In the event of cross-border cybercrime, information should be exchanged as soon as possible. As a result, member countries should make every effort to initiate network security steps as soon as possible.

³⁷ R.K. Suri & T.N. Chhabra, *Cyber Crime* 279 (Pentagon Press, 2004).

³⁸ G-8 countries are USA, UK, Canada, France, Germany, Italy, Japan and Russia.

Internet Treaty by Council of Europe, 2001:

The Council of Europe has been working to counter the increasing international concern about hacking and other computer-related crimes since the 1980s. The Council of Europe's member states unanimously agreed that an international cooperation to combat cybercrime must be genuine, reciprocal, and cooperative in order to achieve the ultimate objective of addressing the issue of internet infrastructure vulnerability. According to the Council of Europe, preserving internet protection faces three major challenges:

- *“Technical difficulties that limit law enforcement agencies' ability to track down and prosecute cyber criminals who work online;*
- *The need for changes to certain substantive and procedural laws that have not kept up with technological advancements, posing legal obstacles to the effective prosecution of cybercriminals;*
- *Infrastructure needs to improve law enforcement agencies' capabilities and ability to keep up with emerging technologies, with a focus on educating people to combat cybercrime.”*

“The Council of Europe considered a new internet treaty in 1997, which was implemented in the form of a text in 2001. Unauthorized access, internet fraud and forgery, child pornography, copyright infringements, and other issues were addressed in the treaty, which required participating countries to establish a specific uniform body of laws to deal with them.” The Council of Europe Treaty proposed legislation to monitor cybercrime activities on a global scale. The treaty was dubbed the International Convention on Cybercrime, and it was aimed at harmonizing national laws that define cybercrime, defining the process for investigating and prosecuting cybercrime in light of global networks, and establishing a fast and efficient international mechanism to tackle cybercrime.³⁹

European Convention on Cyber Crime, 2001:⁴⁰

On November 23, 2001, it was held in Budapest. The aim of this Convention was to consider the changes brought on by the digitalization, integration, and continued globalization of computer networks, as well as the risks that these computer networks and

³⁹ Kamshad, *supra* note 34.

⁴⁰ Convention on Cybercrime, ETS No. 185

electronic information were generating in the form of modes and methods for the perpetration of cybercrimes.

International Conference on E-Security, Cyber Crime & Law, 2004:

On the 19th and 20th of February, “2004, an international conference on e-security, cybercrime, and law was held in Chandigarh, India.” The following were the key topics for discussion at the Conference:

- Network protection for corporate governance and industrial intrusions, as well as network operator hacking liability, which needed a fresh approach;
- New data and transmission standards, as well as encryption methods, were needed. The protection of data banking and electronic fund transfers were also discussed at the meeting;
- Electronic forensics, the protection of computer data, and police procedures for obtaining evidence all needed re-orientation and proper attention;
- The delegates emphasized the importance of cyber law, data security, and relevant legislation for the purpose. The conference also covered topics such as policing cyberspace, “*the role of the judiciary in the digital age, network security and law, and public interest in cybercrime prevention.*”⁴¹

International Cyber Crime Conference, Ukraine, 2004:

On May 26-28, 2004, “*the Computer Crime Research Centre, in cooperation with the World Anti-Criminal and Anti-Terrorist Forum*”, hosted an international conference at Zaporozhe State University in Ukraine. Cyber terrorism, the battle against cybercrime, IPR breaches, piracy, and legal aspects of information security were among the topics discussed at the Conference.⁴²

ASEAN Regional Forum, 2004:

On January 8, 2004, the Association of Southeast Asian Nations (ASEAN) held a high-level ministerial meeting on transnational crimes in Bangkok (China), acknowledging the need for effective legal cooperation to tackle the growing threat of cybercrime in Asia's

⁴¹ Nikita Goel, *A Comprehensive study of cyber security & e – surveillance*, Legal Service India, <http://www.legalserviceindia.com/legal/article-429-a-comprehensive-study-of-cyber-security-and-e-surveillance.html>.

⁴² Kamshad, *supra* note 34.

southeast. The ASEAN Regional Forum released a statement in July 2006 reaffirming its commitment to fighting the rising threat of cyberspace crime by expanding shared cooperation in legal and other areas of mutual concern. The focus of the discussion was on the numerous issues and challenges that come with investigating cybercrimes, as well as the steps that can be taken to combat this ever-increasing evil.

APEC, 2004:

The Asia Pacific Economic Cooperation (APEC) members convened a conference to develop a comprehensive legal structure for the prevention and control of cybercrime, as well as for the strengthening of cyber security, in compliance with established international law principles. It was decided at the ministerial meeting in Santiago (Chile) in November 2004 to improve economic cooperation in the fight against cybercrime.⁴³

11th Congress on Prevention of Crime & treatment of Offenders, 2005:

“The Eleventh Congress on Crime Prevention and Criminal Treatment was held in Bangkok from April 18 to 25, 2005.” It was recognized that current national laws were insufficient to combat the ever-increasing trend of cybercrime on a global scale. As a result, the participating countries needed to work together on a bilateral, regional, and international level to deter crime and improve the criminal justice system.⁴⁴

International Cyber Crime Conference, Brazil, 2006:

The International Cybercrime Conference, held in Brazil from November 6 to 9, 2006, was the 3rd major international gathering in which hundreds of computer experts debated computer crime issues and prevention measures. Electronic and online crime, a 21st-century crime task force model, a critical infrastructure protection program, cyber security, underground hacking operations, criminal file sharing on the internet, cybercrime in an international context, and the need for greater international cooperation in cybercrime investigation and extradition of cyber criminals were among the topics discussed.⁴⁵

⁴³ Kamshad, *supra* note 34.

⁴⁴ *Id.*

⁴⁵ *Id.*

Seventh International Conference on Cyber Crime, 2007:

On September 12, 2007, the Vigyan Bhawan in Delhi (India) hosted the Seventh International Conference on Cyber Crime.⁴⁶ The importance of raising cyber security awareness and developing effective preventive measures to tackle cybercrime was stressed at the conference. The conference's focus was on computer-generated terrorist activities and organized crime through the internet, which criminals have discovered to be a lucrative means of generating large sums of money in a short amount of time. It was widely accepted that online child pornography, contraband trafficking, and e-commerce frauds are on the rise, and that acts of vandalism and cheating were thwarting e-governance efforts. As a result, the urgency of the situation necessitates prompt responses to Interpol referrals and bilateral queries, open sharing of forensic technologies, and further cross-country training exchange programs, as well as timely alerts to effectively combat the cybercrime threat.

International Conference on Terrorism and Organized Crimes, 2008:

On August 25, 2008, an international conference on terrorism and organized crime was held in Anaheim, California. International and domestic terrorism, the misuse of weapons of mass destruction, organized crime, human smuggling and trafficking, identity theft, online drug trafficking, international money laundering, e-commerce, cyber frauds, and computer forensics were all discussed. The conference focused on the widespread use of forensics in cyber-crime cases, as well as the role of computer experts in the investigation process.⁴⁷

Third International Conference on Security and Privacy Issues in Information Technology, 2008:

On September 3, 2008, this conference was held in Prague, Czech Republic. The topic of discussion was hot topics in information technology and the prevention of criminal activity resulting from advancements in this area. There was agreement on the importance of developing “*an international legal strategy to protect national security and personal privacy*”, especially among computer users.⁴⁸

⁴⁶ Anjali Rego, *India Hosts World Cyber Crime Conference*, Firstpost (Sep 12, 2007), <https://www.firstpost.com/tech/news-analysis/india-hosts-world-cyber-crime-conference-3557469.html>.

⁴⁷ Nikita, *supra* note 40.

⁴⁸ Kamshad, *supra* note 34.

Conference on Cyber Security Protective Strategies, 2009:

On November 2-3, 2009, Gatineau hosted an international conference on cyber security and protective strategies (Quebec). The delegates decided that more security measures were needed to address the new threats they were facing as a result of the growing threat of cybercrime. On October 19-21, 2009, a Conference on Cybercrime Security Control System was held in Washington, DC, prior to the Quebec meeting. The conference looked at the security steps taken by member countries and stressed the need for more collaboration and coordination in the battle against cybercrime. On June 18-23, 2009, in Athens (Greece), a conference on Emerging Security Information Systems and Techniques was held to review the steps taken by participating countries to improve their intelligence security informatics.⁴⁹

International Conference on Digital Forensics and Cybercrime, 2009:

It was decided on October 2, 2009, that a standardized pattern of forensic mechanisms should be established to combat digital-related cybercrime. The Conference on Digital Forensics Security and Digital Law, which took place in Pretoria (South Africa) on July 22-24, 2009, was held prior to this one. It was decided that sensitive information exchanged over the internet and by computer systems should be shielded from cyber-attacks. Spoofing is a common tactic used by cyber criminals to obtain data and digital information. Cybercrime involving digital copying or piracy, in particular, necessitates a robust digital security strategy. The needs to update digital law to include both civil and criminal penalties for breaches of digital forensics are also a major concern in order to help investigators better understand crimes involving digital violations.⁵⁰

Fifth Annual Conference on Cybercrime, Council of Europe, 2010:

This conference took place on March 25, 2010 in Strasbourg, France. The conference's main focus was on the following two big issues:

- Fighting online child pornography;
- Networking networks, and so on, in order to improve information technology security and effectively fight cybercrime.

⁴⁹ Kamshad, *supra* note 34.

⁵⁰ *Id.*

Participants were unanimous in their belief that current legislative reforms aimed at preventing and controlling cybercrime and ensuring e-security should continue. The majority of participants agreed that many countries have the global capacity to implement initiatives to tackle web-based crime, and that confidence in information and communication technology must be improved. However, the focus should be on protecting privacy and confidentiality, which are vulnerable to cyber-attacks aimed at stealing data related to financial, industrial, technological, or defense-related computer programs. In light of the fact that internet jurisdiction entails the involvement of numerous parties around the globe whose place of residence and cause of action is shrouded in confusion and defies precise violation and remedial measures, the delegates expressed a common concern for strengthening e-security by extending legal protection to databases and digital information.

UN Congress on Crime Prevention, April 2010:

“It provided an opportunity for the participating countries to reinforce earlier global responses to the threat of cybercrime. The member countries decided to launch a crusade against cyber criminals, particularly cross-border terrorists and foreign perpetrators of cyber fraud.”⁵¹

Fourth International Conference on Cyber Law, August 2010:

On the 18th and 20th of August, 2010, it was held in Virginia (US). The conference focused on cyberspace-related intellectual property rights, privacy protection, and the advancement of computer forensics to tackle transnational cybercrime. These periodic international conferences/congresses indicate that the international community is working hard to monitor and deter cybercrime. Many nations, however, have adopted their own domestic cyber regulations.⁵²

3.4 Information Technology Act, 2000:

The Information Technology Act of 2000⁵³ and the Information Technology Amendment Act of 2008⁵⁴ have been thoroughly examined, and other laws relating to cybercrimes have been briefly addressed. Criminality is both a social and economic problem.

⁵¹ UN, *12th UN Congress on Crime Prevention & Criminal Justice*, (Apr 18, 2010), <https://www.un.org/en/conf/crimecongress2010/>.

⁵² Kamshad, *supra* note 34.

⁵³ The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).

⁵⁴ *The Information Technology Amendment Act, 2008*, [https://police.py.gov.in/Information%20Technology%20Act%202000%20-%202008%20\(amendment\).pdf](https://police.py.gov.in/Information%20Technology%20Act%202000%20-%202008%20(amendment).pdf).

It dates back to the dawn of human civilization. Many ancient books and mythological tales, dating back to prehistoric times, have spoken of crimes committed by individuals, whether against another person, such as robbery and burglary, or against the government, such as espionage and treason. The Arthashastra of Kautilya, written about 350 BC and considered an authentic administrative treatise in India, addresses various crimes, security measures to be taken by rulers, potential crimes in a state, and advocates punishment for a list of specified offences. For the mentioned offenses, various penalties have been prescribed, and the principle of restitution of damage to the victims has also been debated. Crime, in any type, has a negative impact on all members of society. Because of the rapid spread of the Internet and the digitization of economic activities in developed economies, cybercrime has risen at a rapid rate. We see computers and other electronic devices pervading human existence as a result of the widespread adoption of technology in almost all aspects of society, from corporate governance and state administration to the lowest level of petty shopkeepers computerizing their billing system. Man cannot go a day without using a device or a cell phone due to the extent of the penetration. The Information Technology Act of 2000, the Information Technology Amendment Act of 2008, and any other Indian legislation do not describe cybercrime. In reality, it can't possibly be. The Indian Penal Code, 1860, and a number of other statutes have elaborated on offenses and crimes, specifying different acts and the penalties for each. As a result, we can characterize cybercrime as a combination of crime and machine. To put it another way, a cybercrime is any offense or crime that involves the use of a device. Even a minor offense like theft or pick-pocketing will fall under the umbrella of cybercrime if the basic data or assistance to the crime is a device or information stored on a computer used (or misused) by the fraudster. The Information Technology Act defines a computer, computer network, data, information, and all other necessary components of a cybercrime, which we will now go through in detail. In a cybercrime, the machine or the data itself is the victim, the object of the crime, or a method used to commit another crime by supplying the appropriate inputs. Many of these types of crimes will fall under the umbrella of cybercrime. In general, and with special regard to banking and financial sector transactions, the Information Technology Act of 2000 and the Information Technology Amendment Act of 2008. Let us discuss the history of such legislation in India, the circumstances under which the Act was passed, and the intent or aims in passing it before going into section-by-section or chapter-by-chapter descriptions of various provisions of the Act.

Genesis of Information Technology Legislation:

The mid-nineties saw a surge in globalization and computerization, with more and more countries computerizing their government and e-commerce exploding. Until then, the majority of foreign trade and transactions were conducted solely through the transmission of documents through post and telex. Until then, the majority of facts and documents were paper evidences and records or other types of hard-copies. With so much foreign trade conducted through electronic communication and email gaining popularity, an urgent and imminent need for recognizing electronic records, i.e. data stored on a computer or an external storage device connected to it, was felt.

The Model Law on Electronic Commerce was adopted by the “*United Nations Commission on International Trade Law (UNCITRAL) in 1996*”⁵⁵. In January 1997, the United Nations General Assembly passed a resolution urging all UN member states to give the said Model Law serious consideration, as it provides for electronic records to be recognized and treated similarly to paper communications and records.

Objectives of the Information Technology Legislation:

In this context, the Government of India enacted the Information Technology Act of 2000, which has the following objectives, as described in the Act's preface.

“To provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as electronic commerce, which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto.”

The Act primarily addresses the following topics:

- Electronic Documents Legal Recognition;
- Digital Signatures Are Legally Recognized;
- Infractions and Offenses;

⁵⁵ *UNCITRAL Model Law on E-Commerce (1996)*, United Nations Commission on International Trade Law, https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_commerce.

- Cybercrime Justice Dispensation Systems.

The Information Technology Amendment Act, 2008:

The Act, which was the country's first legislation on technology, computers, ecommerce, and e-communication, was the subject of lengthy debates, in-depth analyses, and thorough critiques, with one arm of the industry calling certain parts of the Act punitive and the other claiming it is too diluted and lenient. There were also several glaring omissions, resulting in investigators depending more and more on the time-tested (one-and-a-half-century-old) Indian Penal Code, also in technology-related cases, with the I.T. Act also being referred to in the process and a preference for the IPC over the ITA. Thus, the need for a comprehensive amendment to the I.T. Act was felt almost immediately in 2003-2004. Major business organizations were consulted, and advisory committees were created to look at the I.T. Act's perceived flaws, compare it to similar legislation in other countries, and make recommendations. Such proposals were analyzed and eventually taken up as a detailed Amendment Act, and after extensive administrative processes, the Information Technology Amendment Act 2008 was introduced in Parliament and passed without much discussion towards the end of 2008 (by which time the Mumbai terrorist attack of November 26, 2008 had occurred). The President signed this Amendment Act on February 5, 2009, and it went into effect on October 27, 2009.

The following are some of the ITAA's notable features:

- Focus on data security;
- Emphasizing the importance of information security;
- Defining what a cyber café is;
- Creating a technology-neutral digital signature;
- Defining sound security standards for corporate employees to obey The function of intermediaries is being redefined;
- Appreciating the Indian Computer Emergency Response Team's contribution;
- Additional cybercrimes, such as child pornography and cyber terrorism, have been included;
- Appointing an Inspector to look into cybercrime (as against the DSP earlier)

Structure of the Act:

The ITA 2000 has 13 chapters and 90 parts (the last four sections). The Act starts with a preamble and descriptions, and then moves on to chapters dealing with electronic record authentication, digital signatures, and electronic signatures, among other things. There are detailed protocols for certifying authorities (for digital certificates as per the IT Act, 2000, which has since been replaced by electronic signatures in the ITAA, 2008). The civil offense of data theft has been identified, as well as the adjudication and appeals processes. The Act then goes on to identify and explain some of the more well-known cybercrimes, as well as the penalties associated with them. The definition of due diligence, the position of intermediaries, and a few other provisions were then discussed. The Act's rules and procedures have also been phased in, with the most recent one on the classification of private and confidential personal data, as well as the role of intermediaries, due diligence, and so on, being established as recently as April 2011.

Applicability:

The Act covers the entire country and also applies to any offence or violation committed outside of India by any individual. The Act has several clear exclusions (i.e., places where it does not apply), which are mentioned below in the First Schedule:

- *“Negotiable instrument (Other than a cheque) as defined in section 13 of the Negotiable Instruments Act, 1881;*
- *A power-of-attorney as defined in section 1A of the Powers-of-Attorney Act, 1882;*
- *A trust as defined in section 3 of the Indian Trusts Act, 1882;*
- *A will as defined in clause (h) of section 2 of the Indian Succession Act, 1925 including any other testamentary disposition;*
- *Any contract for the sale or conveyance of immovable property or any interest in such property;*
- *Any such class of documents or transactions as may be notified by the Central Government.”*

Digital & Electronic Signature:

The ITAA, 2008 specified electronic signature, while the earlier ITA, 2000 defined digital signature in detail, identifying it and elaborating the process for obtaining a digital

signature certificate and granting it legal validity. The ITA, 2000 described digital signatures as "authentication of electronic record" according to the procedure outlined in Section 3, and Section 3 discussed the use of asymmetric crypto systems, Public Key Infrastructure, and hash functions, among other things.

Later, this was criticized as being technology-dependent, i.e., depending on the basic technology of an asymmetric crypto scheme and the hash function to generate a pair of public and private key authentication, among other things. Thus, in ITAA, 2008, Chapter II was renamed from Digital Signature to Digital Signature and Electronic Signature⁵⁶, incorporating technical neutrality through the introduction of electronic signatures as a legally legitimate mode of executing signatures. This involves digital signatures as one of the signature types, but it goes far further in scope, including biometrics and other new ways of producing electronic signatures, rather than limiting recognition to the digital signature process alone. Though TCS, Safe script, and MTNL are some of India's digital signature certifying authorities, IDRBT (Institute for Development of Research in Banking Technology – the RBI's research arm) is the Certifying Authorities (CA) for the Indian banking and financial sector, as authorised by the Controller of Certifying Authorities.

It's important to know what a digital signature (or electronic signature) is in this context. It's important to remember that an electronic signature (or, in the past, a digital signature) as described by the Act is not the same as a digitized or scanned signature. In reality, there is no real signature by the individual in the traditional sense of the term in an electronic signature (or digital signature). The method of storing or scanning one's signature and submitting it in an electronic correspondence such as email is not considered an electronic signature. It is a method of message authentication based on the protocol outlined in Section 3 of the Act.

Other ways of authentication that is easier to use, such as biometric based retina scanning, can be very useful in ensuring that the Act is implemented effectively. The Central Government, on the other hand, must develop comprehensive procedures and raise public knowledge about the use of such systems by putting in place the required resources and stipulating necessary conditions. Furthermore, the responsibilities of electronic signature certificate issuing authorities for biometric-based authentication mechanisms must be

⁵⁶ The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India), S. 3A.

established, as well as the required criteria to make it user-friendly while maintaining protection.

E Governance:

The legal recognition of electronic records⁵⁷ is discussed in Chapter III and accompanied by a summary of procedures for “electronic records, storage, and maintenance, and the recognition of the validity of contracts established by electronic means.”

The parts that follow detail the procedures for electronic signatures as well as regulatory guidance for certifying authorities.

Penalties, Restitution, and Adjudication (Chapter IX) is a big step forward in mitigating data theft, claiming compensation, introducing security practices which deserve a thorough summary.

Section 43:⁵⁸ This section represents India's first big and important legislative move in combating data theft. The IT industry has long argued that data fraud, including physical theft or larceny of goods and services, should be addressed by legislation in India.

Theft of data is a civil offense addressed in this section. If a person accesses or installs, copies, or extracts any data from a computer without the permission of the owner or another person in control of the computer, or introduces any computer contaminant such as a virus, or damages or disrupts a computer, or denies access to a computer to an authorized user, or tampers, he is liable to pay damages to the person so affected. The maximum damages under this heading were previously set at Rs.1 crore in the ITA-2000, but this (the ceiling) was removed in the ITAA 2008.

This section is all about civil liability. The criminality of data theft will be dealt with separately later under Sections 65⁵⁹ and 66⁶⁰. Writing a virus program or sending a virus email, installing a bot, a Trojan, or some other malware in a computer network, or triggering a Denial of Service Attack on a server all fall under this section which may result in civil liability. Computer Virus, Compute Contaminant, Computer Database, and Source Code are all listed and specified in this section.

⁵⁷ The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India), S. 4

⁵⁸ Penalty and Compensation for damage to computer, computer system, etc.

⁵⁹ Tampering with Computer Source Documents.

⁶⁰ Computer Related Offences.

In court cases like the bazee.com case and others, questions like the workers' liability in an organization suing for data manipulation or other offenses, the amount of responsibility of the employer or the owner, and the definition of due diligence were all discussed in the first few years of ITA, 2000. As a result, the need to define corporate responsibility for data protection and information security at the corporate level became apparent.

As a result, in the ITAA, 2008, a new Section 43-A⁶¹ was added. This is yet another landmark moment in the field of data security, especially at the corporate level. According to this Section, if a body corporate fails to enforce fair security practices and thereby causes undue harm or gain to an individual, the body corporate will be liable to pay damages as compensation to the person affected. The section also defines the terms body corporate and fair security policies and procedures, as well as sensitive personal data or information.

Thus, by adding Section 43A, which requires corporations to ensure the adoption of fair security standards, the corporate responsibility for data protection is greatly emphasized. Furthermore, the central government explained what constitutes sensitive personal data in its Notification dated April 11, 2011, which included a list of all such data, including passwords, bank account or card information, medical records, and so on. Following this notification, the IT industry in the country, including tech-savvy and heavily technology-based banking and other sectors, became acutely aware of the importance of data protection, and a general understanding of what data privacy is and the role of top management and the Information Security Department in organizations in ensuring data protection, especially when handling sensitive data, grew.

The Government of India, Department of Information Technology, notified the Information Technology (Reasonable security practices and procedures and confidential personal data or information) Rules on April 11, 2011. Anybody corporate or a person acting on its behalf shall be deemed to have followed reasonable security practices and procedures if they have implemented such practices and standards and have a comprehensive documented information security program and policies including managerial, technical, operational, and physical security control measures commensurate with a reasonable level of risk. In the event of an information security violation, the body corporate or an individual acting on its behalf must show, when and when necessary by the law enforcement agency, that security control measures have been enforced in accordance with their documented information security

⁶¹ Compensation for failure to protect data.

program and policies. As a result of the above, it has now become a major compliance problem for not only IT companies, but also those in the Banking and Financial Sector, especially those banks that have large computerized operations that deal with public data and rely heavily on technology. In the event of a lawsuit or a security violation resulting in a claim for financial loss or damages, it will be the body corporate's massive duty to show that the above-mentioned Reasonable Security Practices and Procedures were still in effect and that all of the measures outlined in the Rules passed in April 2011 had been taken.

This is one of the parts that will generate a lot of noise and be the focus of a lot of debates in the near future, such as redefining the role of an employee, the duty of an employer or top management in data security, and issues like actual and vicarious responsibility, actual and contributory negligence of all stakeholders involved, and so on. The problem has broader implications, particularly in the case of cloud computing (the practice of storing, managing, and processing data using a network of remote servers hosted on the Internet rather than a local server, with services managed by the provider sold on demand, for the amount of time used), where more and more organizations handle the data of others and the information is stored on the cloud. More debates are likely to arise over the issue of information owners versus information containers and custodians, and the Service Level Agreements of all parties concerned will become more relevant.

Adjudication:

After discussing civil offenses, the Act goes on to define a civil remedy for such offenses in the form of adjudication, which can be obtained without having to file a report with the police or other investigative agencies. The powers and procedures of adjudication have been detailed in Sections 46⁶² and later. As adjudicator, the Central Government can designate any officer of the Government of India or a state government who is not below the rank of director. In most states, the I.T. Secretary is the designated Adjudicator for all civil offenses arising from data thefts and the resulting damages. If there is one part of the IT Act that can be criticized for being completely unpopular, it is this one. Just a few applications were filed in the first ten years of the ITA's existence, and almost all of them were in the major metros, almost all of which are in various stages of the judicial process, with adjudications received in maybe less than five instances. In April 2010, the first adjudication under this clause was obtained in Chennai, Tamil Nadu, in a case involving ICICI Bank, in

⁶² Power to Adjudicate.

which the bank was ordered to pay the claimant for the amount wrongfully debited in Internet Banking, as well as costs and damages.

This section should be given a lot of attention, and the public, especially victims of cybercrime and data theft, should be made aware that such a procedure exists without having to go to the police and file a complaint. It's past time for the state to devote some time and thought to raise public consciousness about the provision of adjudication for civil offenses in cyber litigations such as data theft, so that the reason for which such valuable provisions have been rendered is effectively used by the litigant public.

Under this process, there is an appeals mechanism, and the structure of the Cyber Appellate Tribunal at the national level is also defined in the Act. Every adjudicating officer has civil court powers, and the Cyber Appellate Tribunal has civil court powers under the Code of Civil Procedure.

"The Act goes on to the individual criminal activities that fall under the wider scope of cybercrimes after discussing the processes relating to appeals and the roles and powers of the Cyber Appellate Tribunal." It's worth noting that the Act only mentions a few cybercrimes (without specifying what constitutes a cybercrime) and specifies the penalties for those offenses. The IT Act's penal laws, including those dealing with cognizable offenses and criminal actions, are included in Chapter IX, "Offenses."

Section 65:⁶³ When computer source code is supposed to be retained or preserved by statute, concealing, damaging, or changing it is a crime punishable by three years in prison or two lakh rupees in fines, or both. Fabrication of an electronic record or forgery by interpolation in a CD created as proof in court are both punishable under this Section.⁶⁴ In this section, "computer source code" refers to any listing of programs, computer commands, design and layout, and so on.

Section 66:⁶⁵ This section refers to the data theft listed in Section 43. Whereas in that section it was merely a civil offense with only compensation and restitution as a remedy, here it is the same crime but with a criminal intent, rendering it a criminal offense. If done dishonestly or fraudulently, the act of data theft or the offence specified in Section 43 becomes a criminal offence under this Section, which carries a sentence of up to three years

⁶³ *Supra* note 58.

⁶⁴ *Bhim Sen Garg v. State of Rajasthan*, 2006 CriLJ 3643.

⁶⁵ *Supra* note 59.

in prison or a fine of up to five lakh rupees, or both. Hacking was previously known as a crime under Section 66 of the Criminal Code.

After the change, data theft is now referred to in Sec 66, making this section more purposeful and excluding the term hacking. The term hacking was previously classified as a crime in this section, and courses on ethical hacking were also offered. As a result, people began to wonder how an immoral activity could be taught academically with the word ethical prefixed to it. Then, for example, will there be training programs on Ethical Theft, Ethical Attack, and so on for courses on physical defense? The ITAA resolved this thorny problem by rewriting Section 66 to align it with Section 43's civil liability provisions and deleting the term hacking. However, according to this Section, hacking is still a crime, even though some experts interpret hacking to mean generally for good reasons (obviously to make naming the courses ethical hacking) and cracking to mean criminal purposes. It's worth noting that the technology used in both is the same, and the act is the same, while in hacking, the owner's permission is sought or suspected, and the latter act of cracking is considered a crime.

Section 66 has been widened as a result of ITAA, which now includes the following offenses:

66A: This section covers sending offensive messages via a contact service, causing annoyance, or sending an email to confuse or deceive the receiver about the origin of those messages (commonly known as IP or email spoofing). These crimes are punishable by up to three years in jail or a fine. This Section was struck down by J. Chelameswar & R.F. Nariman in the Case *Shreya Singhal v. Union of India*⁶⁶.

66B: Receiving a stolen computer resource or communication device with a penalty of up to three years in prison or a fine of one lakh rupees, or both.

66C: Electronic signatures or other forms of identity fraud, such as stealing someone else's password or electronic signature, and so on. Three years in jail or a fine of one lakh rupees, or both, is the penalty.

66D: Cheating by impersonation using a computer resource or a communication device is punishable by imprisonment of either description for a period of up to three years, as well as a fine of up to one lakh rupees.

⁶⁶ *Shreya Singhal v. Union of India*, AIR 2015 SC 1523.

66E Breach of privacy: Publishing or distributing a person's private information without their permission, etc. Three years in jail or a fine of two lakh rupees, or both, is the penalty.

66F Cyber terrorism: Threatening the nation's unity, dignity, protection, or sovereignty by refusing access to someone who is allowed to use a computer resource or attempting to penetrate or access a computer resource without permission. This section covers acts that result in a computer contaminant (such as a virus, Trojan horse, or other spyware or malware) that is likely to cause death or injury to people, as well as property damage or destruction. The penalty is life in prison.

“All actions under S.66 are cognizable and non-bailable offenses, as can be seen. The presence of criminal purpose and the evil spirit, i.e. the principle of mens rea, destruction, deletion, modification, or diminishment of the value or usefulness of data, are all major ingredients to bring any act under this Section.”

To summarize, what was formerly a civil liability with the right to restitution and damages under Section 43 has now been referred to as a criminal liability punishable by imprisonment, fines, or both if committed with criminal intent.

Section 67: It deals with the electronic publication or transmission of pornographic content. *“The earlier section of the ITA was later widened as part of the ITAA 2008, which included child pornography and the preservation of information by intermediaries.”*

This section deals with publishing or distributing obscene content in an electronic format. Whoever publishes or transmits any material that is lascivious or appeals to the prurient interest, or whose effect is such that it tends to deprave and corrupt persons who are likely to read the matter contained in it, shall be punished with a first conviction for a term up to three years and a fine of five lakh rupees, or both.

This Section is historically significant because it was in this Section that the landmark judgment in what is widely regarded as India's first ever conviction under the I.T. Act 2000 was handed down on November 5, 2004 in the famous case State of Tamil Nadu v. Suhas Katti.⁶⁷ The prosecution proved the Section's intensity and the reliability of electronic evidences in this case, which included sending obscene messages in the name of a married

⁶⁷ State of Tamil Nadu v. Suhas Katti, CC No. 4680 of 2004.

woman, which amounted to cyber harassment, email spoofing, and the criminal activity mentioned in this Section.⁶⁸

Section 67-A: It deals with the electronic publication or transmission of content involving sexually explicit acts. Where the contents of Section 67 are combined with sexually explicit material, a penalty is imposed under this section.

Child Pornography:⁶⁸ This section includes depicting children engaging in sexually explicit acts, producing text or digital images, advertising or encouraging such material depicting children in an obscene or pornographic manner, or enabling child abuse online or causing children to participate in online relationships with one or more children. For the purposes of this Section, children refer to people who have not reached the age of eighteen. A first conviction carries a maximum sentence of five years in prison and a fine of ten lakh rupees, while a second conviction carries a sentence of seven years in prison and a fine of ten lakh rupees.

To ensure that printing and distribution of ancient epics or heritage content, as well as pure scholarly books on education and medicine, are not adversely affected, this Section expressly excludes bonafide heritage material being printed or circulated for the purpose of education or literature. Making pornographic video or MMS clippings or sharing such clippings through mobile or other means of communication through the Internet fall under this category, as do screening video graphs and photographs of illegal activities through the Internet.

Section 67C: It assigns intermediaries the duty of preserving and retaining defined information for the period and in the manner prescribed by the Central Government. Noncompliance is a crime punishable by up to three years in jail or a fine.

Section 69: This is a fascinating section because it allows the government or specified agencies to intercept, track, or decrypt any information produced, distributed, obtained, or stored in any computer resource, subject to the procedures outlined here. This power may be used if the Central Government or the State Government, as the case may be, believes it is essential or expedient in the interests of India's sovereignty or integrity, defense, security, friendly relations with foreign states, or public order, or to prevent incitement to commit any cognizable offence relating to the above, or to invest. In any such event, the

⁶⁸ The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India), S. 67-B

required procedure must be followed, and the reasons for taking such action must be recorded in writing by order directing any agency of the appropriate government. When requested, the subscriber or intermediary must provide all facilities and technical assistance.

“The ITAA was amended to include Section 69A, which gives the Central Government or any of its officers the authority to issue directions prohibiting public access to any information through any computer resource, under the same conditions as described above. The power to authorize the monitoring and collection of traffic data or information via any computer resource is discussed in Section 69B.”

Due Diligence:

In Section 79, intermediary liability and the principle of Due Diligence is discussed. As a result, if his role is limited to providing access to a communication system over which information made available by third parties is transmitted, temporarily stored, or hosted, or if he does not initiate the transmission, select the receiver of the transmission, or select or modify the information contained, the intermediary shall not be liable for any third party information hosted by him.

The principle of due diligence is also a hot topic of discussion. Due Diligence was first debated as a direct result of the well-known bazee.com case in New Delhi, in which the company's NRI CEO was arrested for making MMS clippings with inappropriate pornographic content depicting school children available for sale on his public domain website (and later the CD was sold). The broader problem at the time was how much responsibility lies with the content provider and how much with the Internet Service Provider, as well as what constitutes due diligence, which he should have exercised as the company's CEO.

On April 11, 2011, the DIT issued a set of rules titled Information Technology (Intermediaries Guidelines) Rules to clarify the meaning of due diligence and what constitutes due diligence following the passage of the ITAA and the implementation of fair security standards and procedures and the duty of the body corporate as seen earlier in Section 43A, and to put to rest any doubt about the significance of due diligence and what constitutes due diligence. According to this, the intermediary, on whose computer system the information is stored, hosted, or released, shall act within thirty-six hours after obtaining knowledge of any such information as mentioned in sub-rule (2) above or being brought to

actual knowledge by an affected person in writing or through email signed with an electronic signature about any such information as mentioned in sub-rule (2) above, shall act in writing or through email signed with an electronic signature about any such information as mentioned in sub-rule (2) above, and where applicable (2). Furthermore, the intermediary must keep those details and related documents for at least ninety days in order to conduct an investigation. In other words, an intermediary will be held responsible for any law violation committed by a consumer unless the Intermediary can demonstrate that he did his due diligence and did not conspire or abet the illegal act.

Section 80 describes the ability to join, browse, and so on. Any police officer not below the rank of Inspector or any other officer authorized may enter any public place and search and arrest without warrant any person found there who is reasonably suspected of having committed, committing, or being about to commit any offence under this Act, notwithstanding anything contained in the Code of Criminal Procedure. This is yet another powerful tool that police officers have only used infrequently, if at all. Electronic and truncated cheques are covered by the Act (i.e. the image of cheque being presented and processed curtailing and truncating the physical movement of the cheque from the collecting banker to the paying banker). In the sections that follow, the Act's overriding powers, as well as the powers of the Central Government to make rules and the powers of state governments to make rules when applicable, are addressed.

Other Acts Amended by the ITA:

1. The Indian Penal Code, 1860:

The Indian Penal Code, or IPC, is a very influential law that serves as India's key criminal code. It is perhaps the most commonly used in criminal jurisprudence. It includes nearly all fundamental elements of criminal law and is supplemented by other criminal provisions. It was first enacted in 1860 and has been revised several times since then. Many special laws have been enacted in independent India with criminal and penal provisions that are often referred to and relied upon as an additional legal framework in situations where the applicable provisions of the IPC are also referred to.

The term electronic was added to the parts of the IPC dealing with records and documents by ITA 2000, effectively treating electronic records and documents on par with physical records and documents. Sections dealing with false entry in a record or false

document (e.g., 192, 204, 463, 464, 468 to 470, 471, 474, 476, etc.) have since been amended as electronic record and electronic document, putting all offences involving an electronic record or electronic document into the ambit of the IPC, much like physical acts of forgery or falsification of physical records.

In practice, however, investigating agencies file cases citing similar sections from the IPC in addition to those corresponding in the ITA, such as offences under IPC 463, 464, 468, and 469 read with ITA/ITAA Sections 43 and 66, to ensure that the proof or penalty mentioned at least in any of the legislations can be easily obtained.

“All of the cyber-crimes under the IPC are bailable other than offences under section 420 (cheating and dishonestly inducing delivery of property), section 468 (forgery for the purpose of cheating), section 411 (dishonestly receiving stolen property), section 378 (theft) and section 409 (criminal breach of trust by public servant, or by banker, merchant or agent), which are non-bailable.”⁶⁹

“Offences under sections 463 and 465 (forgery), sections 425 and 426 (mischief), section 468 (forgery for the purpose of cheating), section 469 (forgery for the purpose of harming reputation) and section 292 (sale, etc., of obscene books, etc.) of the IPC are non-compoundable offences while offences under sections 378 and 379 (theft), 420 (cheating and dishonestly inducing delivery of property), sections 425 and 426 (mischief when the only loss or damage caused is loss or damage to a private person), section 509 (word, gesture or act intended to insult the modesty of a woman), section 411 (Dishonestly receiving stolen property) and section 419 (Punishment for cheating by personation) of the IPC are compoundable offences. Of these, offences under sections 420 and 509 can be compounded only with the permission of the court. Most of the cyber-crimes under the IPC are cognizable other than the offences under sections 425 and 426 (mischief) and sections 463 and 465 (forgery) which are non-cognizable.”⁷⁰

“The overlap between the provisions of the IPC and the IT Act may sometimes lead to an anomalous situation wherein certain offences are bailable under the IPC and not under the IT Act and vice versa and certain offences are compoundable under the IPC and not under the IT Act and vice versa. For instance, in case of hacking and data theft, offences

⁶⁹ Vinod Joseph & Deeya Ray, *Cyber Crimes under the IPC & IT ACT: An – Uneasy Co-existence*, Mondaq (Feb 10, 2020), <https://www.mondaq.com/india/it-and-internet/891738/cyber-crimes-under-the-ipc-and-it-act--an-uneasy-co-existence>.

⁷⁰ Vinod, *supra* note 67.

*under sections 43 and 66 of the IT Act that are bailable and compoundable while offences under section 378 of the IPC are non-bailable and offences under section 425 of the IPC are non-compoundable. Further, in case of the offence of receipt of stolen property, the offence under section 66B of the IT Act is bailable while the offence under section 411 of the IPC is non-bailable. Similarly, in case of the offence of identity theft and cheating by personation, the offences under sections 66C and 66D of the IT Act are compoundable and bailable while the offences under sections 463, 465 and 468 of the IPC are non-compoundable and the offences under sections 468 and 420 of the IPC are non-bailable. Finally, in case of obscenity, the offences under sections 67, 67A and 67B of the IT Act are non-bailable while the offences under section 292 and 294 of the IPC are bailable.*⁷¹

2. The Indian Evidence Act, 1872:

The ITA has changed yet another piece of legislation. Prior to the enactment of the ITA, all testimony in a court was only in physical form. With the ITA recognizing all electronic records and documents, it was only reasonable that the country's evidentiary laws be updated to reflect this. The words "all papers, including electronic records" were substituted in the Act's definitions section. Words like "digital signature," "electronic form," "safe electronic record," and "metadata," as used in the ITA, were introduced to make them part of the evidentiary process in laws.

The Act's Section 65B, which establishes the admissibility of electronic records as evidence, is important. This is a lengthy section that serves as a watershed moment in the field of evidence produced by a computer or electronic device. If the following requirements are met, any information found in an electronic record printed on paper, stored, recorded, or copied in optical or magnetic media created by a machine shall be regarded as a text, without further proof or development of the original:

- During the time in which the machine was frequently used by lawful persons, the computer output containing the information was provided by the computer;
- The information obtained was fed into the machine on a regular basis as part of the said activities;
- The machine was operational for the majority of the time span, and a certificate signed by a responsible individual, etc.

⁷¹ Vinod, *supra* note 67

To put it another way, evidences (information) obtained from computers or electronic storage devices and printed or stored on electronic media are valid if they were obtained from a system that was properly handled, with no room for data manipulation and ensuring data integrity, and accompanied by a certificate signed by a responsible person.

However, one segment of the industry often misinterprets this section to mean that computer printouts can be used as proof and are legitimate as proper documents even though they are not signed. Many computer generated letters from large corporations have a signature space below the words Your faithfully or truly, with the signature space left vacant and a Post Script comment at the bottom. This is a computer generated letter and therefore does not require signature. The Act makes no mention of the fact that computer print-outs do not need to be signed and can be used as a record.

3. The Banker's Books Evidence Act, 1891:

The third schedule of the ITA contains amendments to this Act. Prior to the passage of the ITA, any testimony from a bank that was to be presented in court required the production of the original ledger or other register for authentication, with the copy being held in the court records as exhibits.

Of short, the provisions in the Bankers Books Evidence Act make a printout from a computer system, a floppy or disc, or a tape, a valid document and evidence, provided that such print-out is accompanied by a certificate stating that it is a true extract from the bank's official records and that such entries or records are from a computerized system with props.

4. The Reserve Bank of India Act, 1934:

“The next Act that was amended by the ITA is the Reserve Bank of India Act, 1934. Section 58 of the Act sub-section (2), after clause (p), a clause relating to the regulation of funds transfer through electronic means between banks (i.e. transactions like RTGS and NEFT and other funds transfers) was inserted, to facilitate such electronic funds transfer and ensure legal admissibility of documents and records therein.”

3.5 Analysis of ITA & ITAA:

After going over all of the provisions of the ITA and ITAA in depth, let's take a look at some of the Act's wider areas of omissions and commissions, as well as some of the general criticism the Acts have received over the years.

There is no serious provision in the Act for raising awareness and putting such measures in place. The government, or investigating agencies such as the Police Department (whose job has been made comparatively easier and focused as a result of the passage of the IT Act), have not taken any serious steps to raise public awareness about the provisions in these statutes, which is absolutely necessary given that this is a new area and technology must be learned by all stakeholders. Many people, including those in the investigating agencies, are unaware of provisions like the nature of the adjudication process.

Jurisdiction: This is a big problem that neither the ITA nor the ITAA adequately discuss. Jurisdiction is stated in Sections 46, 48, 57, and 61 in connection with the adjudication process and the appeal procedure, and again in Section 80 as part of the police officers powers to enter and search a public place for a cybercrime, among other things. Sections 13 (3) and (4) of the Electronic Records Act address the location of electronic record dispatch and reception, which may be interpreted as jurisprudence problems.

However, some fundamental issues remain, such as which police station does the accused go to if his mail is hacked and he is a resident of a city in another state when he learns of it in a different city? Where does an employee of a multinational corporation with branches across the world and in many Indian metropolises go to file a complaint if he suspects another person, say an employee of the same corporation, in his branch or headquarters office and tells the police that evidence might be found on the suspect's computer system? Sometimes, prosecutors refuse to consider such charges due to a lack of jurisdiction, and judicial officers have also been unable to deal with such cases. The awareness that cybercrime is geographically agnostic, borderless, territory-free, and devoid of all authority and frontiers, and occurs in the cloud or room, must be widely disseminated, and proper training must be given to all involved players in the sector.

Evidence: In cybercrime, evidence is a big concern. The 'crime scene' problems are the pat of evidences. There is no such thing as cybercrime. We can't mark a location, a device, or a network, and we can't instantly seize the hard drive and hold it under lock and key like an exhibit taken from the crime scene.

In the world of cybercrime, almost everything can be used as a scene! The crime scene consists of the evidences, data, network, and related devices, as well as the log files and trail of events originating or documented in the system. Many times, evidences which lie in some device, such as the intermediaries' computers or the opponent's computer system, while

filing cases under the IT Act, whether it is a civil case in the adjudication phase or a criminal complaint filed with the police. In both of these scenarios, crucial information may be easily lost unless the police move quickly to seize the systems and capture the evidence. In fact, if one thinks his machine is going to be seized, he will immediately begin destroying proof (formatting, deleting history, deleting cookies, modifying the registry and user login setups, reconfiguring system files, and so on) because most computer history and log files are volatile.

In India, there is no major initiative on common repositories of electronic evidences by which, in the event of any dispute (including civil), the affected computer may be handed over to a common trusted third party with proper software tools, who may keep a copy of the entire disk and return the original to the owner, allowing him to use it at his leisure while the copy is produced as evidence. There are software tools available for this, such as EnCase, which has a global reputation, and our own C-DAC tools, which have extensive retrieval capabilities, search functionality without allowing for additional writing, and the preservation of the original version with a date stamp for production as proof.

Many offences are not covered: Unlike many Western countries and some smaller East Asian countries, India only has one set of laws: the ITA and ITAA. As a result, many cyber-crime problems, as well as many crimes in general, are left unaddressed. Many cyber-crimes, such as cyber-squatting, are carried out with the intent of extorting money. Spam emails, ISP responsibility for copyright infringement, and data protection concerns have not been adequately addressed.

Furthermore, the majority of Indian corporations, including some government-owned enterprises, use operating systems from the West, especially the United States, and many software utilities, hardware, and firmware are imported from abroad. In such cases, the actual scope and import of IT Act Sections dealing with utility software, system software, or an Operating System modification or update used for installing the software utility must be discussed explicitly, because otherwise, the user does not know if the upgrade, patch, or spyware is being downloaded or installed. The Act does not discuss the government's policy on corporate backups, like PSUs and PSBs, being stored in our country or abroad, or the arbitrary legal jurisprudence on such software backups if they are kept abroad.

As mentioned earlier in the chapter, the majority of cybercrimes in the country are still prosecuted under the related parts of the IPC in conjunction with the comparative

sections of the ITA or the ITAA, giving investigators the assurance that even if the ITA portion of the case is missing, the accused cannot escape the IPC part.

To quote the noted cyber law expert in the nation and Supreme Court advocate Shri Pavan Duggal, *“While the lawmakers have to be complemented for their admirable work removing various deficiencies in the Indian Cyber law and making it technologically neutral, yet it appears that there has been a major mismatch between the expectation of the nation and the resultant effect of the amended legislation. The most bizarre and startling aspect of the new amendments is that these amendments seek to make the Indian cyber law a cyber-crime friendly legislation; a legislation that goes extremely soft on cyber criminals, with a soft heart; a legislation that chooses to encourage cyber criminals by lessening the quantum of punishment accorded to them under the existing law; a legislation which makes a majority of cybercrimes stipulated under the IT Act as bailable offences; a legislation that is likely to pave way for India to become the potential cybercrime capital of the world.”*⁷²

Let us not be cynical and believe that current law is favorable to cyber criminals or that it would lead to a rise in crime. Without a doubt, it does not. It is a commendable piece of legislation, a significant first move and a significant milestone in the nation's technological development. But let us not be fooled into thinking that the current law would suffice. It's important to note that criminals are still one step ahead of investigators in terms of technology. After all, in the Parliament Attack case, steganography was used to send a one-line coded message from one suspect to another, which served as a lesson for the investigators to learn more about the technology of steganography. Satellite phones were also used in the Mumbai attack case in November 2008, which alerted investigators to the technical risks of such devices, as they had previously relied solely on mobile phones, directional monitoring by cell phone towers, and Call Details Register entries. Hopefully, more public awareness campaigns will be conducted, and the government will be mindful of the need to enact additional legislation. More laws might not be enough, since the conviction rate for cyber-crime offenses is among the lowest in the nation, much lower than the rate for IPC and other offenses. The government should be mindful that it is the assurance of punishment, not the severity of punishment that acts as a deterrent to offenders. It is the guarantee of punishment that the legislation can offer, not the number of laws in a country, which can deter crimes.

⁷² Pavan Duggal, *Cyber Law* (Universal Law Publishing, 2nd ed., 2018).

3.6 Conflicts between ITA & IPC:

The controversy between the IPC and the IT Act was highlighted in the case of Sharat Babu Digumarti v. Government of NCT of Delhi⁷³. In this case, an obscene video was classified for sale on baazee.com on November 27, 2004. To avoid detection by Bazees filters, the listing was put under the category 'Books and Magazines' and the sub-category eBooks. Before the listing was taken down, a few copies were sold. Avinash Bajaj, Bazees managing director, and Sharat Digumarti, Bazees manager, were later charged by Delhi police's crime division. Since Avinash Bajaj's employer, Bazees, was not named as a defendant, the court ruled that vicarious liability could not be imposed on him under either section 292 of the IPC or section 67 of the IT Act because Avinash's employer, Bazees, was not named as a defendant. Later, the charges against Sharat Digumarti under section 67 of the IT Act and section 294 of the IPC were dismissed, but the charges under section 292 of the IPC were held. The Supreme Court then considered whether a claim under section 292 of the IPC could be upheld after the charges under section 67 of the IT Act were dismissed. The charges against Sarat Digumarti were quashed by the Supreme Court, which ruled that if an offence requires an electronic record, the IT Act alone must apply because that was the legislative intent. It is a well-established rule of understanding that special laws will take precedence over general laws, and that later laws will take precedence over previous legislation. Furthermore, section 81 of the IT Act states that the provisions of the IT Act will apply notwithstanding anything in any other legislation currently in force that is inconsistent with them.⁷⁴

Certain persons were accused of stealing data and software from their employer and charged under sections 408 and 420 of the IPC, as well as sections 43, 65, and 66 of the IT Act, in the case of Gagan Harsh Sharma v. The State of Maharashtra⁷⁵. With the exception of section 408 of the IPC, all of these parts have already been discussed. *"Whoever, being a clerk or servant or employed as a clerk or servant, and being in any manner entrusted in such capacity with property, or with any dominion over property, commits criminal breach of trust in respect of that property, shall be punished with imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine"*.⁷⁶

⁷³ Sharat Babu Digumarti v. Government of NCT of Delhi, AIR 2017 SC 150.

⁷⁴ Vinod, *supra* note 67.

⁷⁵ Gagan Harsh Sharma v. The State of Maharashtra, 2019 CriLJ 1398.

⁷⁶ Vinod, *supra* note 67.

Non-bailable offenses under sections 408 and 420 of the IPC can only be compounded with the approval of the court. Sections 43, 65, and 66 of the IT Act provide for bail and compounding of offenses. As a result, the petitioners requested that the IPC charges against them be dismissed and that the IT Act charges against them be reviewed and pursued. It was also argued that if the Supreme Court's ruling in Sharat Babu Digumarti was followed, the petitioners could only be sued under the IT Act, not the IPC, for the same conduct.⁷⁷

“The Bombay High Court upheld the petitioners' arguments and ordered that the IPC charges against them be dismissed.”

3.7 Prevention of Money Laundering Act, 2002:

In every emerging economy, black money has always been a serious problem. Nation builders, legislators, and particularly the country's financial administrators have always worked hard to combat the evils of black money and other illegally obtained profits. The Anti Money Laundering Act of 2002⁷⁸ is a big step in this direction in India. One of the Act's key goals was to allow for the confiscation of property arising from or involved in money laundering.

Money laundering, while not specified in the Act, may be interpreted to mean attempting to engage in any process or operation related to the proceeds of crime and projecting it as untainted property, whether directly or indirectly. Money laundering is punishable by rigorous imprisonment for a period of not less than three years but not more than seven years, as well as a fine of up to five lakh rupees, according to the Act.

Money laundering is the method of obtaining funds from illicit sources, layering them in legitimate sources, incorporating them into legal systems such as banking, and then using them. Since the banking industry plays such a large and important role in money laundering, banks now have a serious duty to ensure that the banking channel is not used in illegal activity. It is now much more than a responsibility; it is also an enforcement concern.

Banks must keep records of all transactions of the nature and value listed in the rules, provide transaction details within the defined time frame when warranted, and check and maintain records of all customers' identities. As a result, adherence to Know the Customer guidelines and the preservation of all KYC records takes on a new level of importance and

⁷⁷ Vinod, *supra* note 67

⁷⁸ The Prevention of Money Laundering Act, 2002, No. 15, Acts of Parliament, 2003 (India).

becomes an enforcement problem. Cash transactions and suspicious transactions must be recorded and documented as required. If any of these requirements are not met, the concerned bank official will be charged with money laundering and will be found guilty under the Act.

Electronic Records Maintenance:

“Computerization began in most Indian banks in the late 1980s in the form of stand-alone systems known as Advanced Ledger Posting Machines (separate PC for each counter/activity), leading to the age of Total Branch Automation or Computerization in the early or mid-1990s. TBA, or TBC as it was more commonly known, marked the beginning of a networked environment on a Local Area Network under client-server architecture, when records were held in electronic form on hard disks and external media such as tapes and other backup media.”

After the passage of the ITA and the identification of electronic records, banks have been required to establish a proper computerized system for electronic records. Traditionally, all legacy structures in banks have a record maintenance policy, which is also approved by the RBI and their respective Boards and specifies the time of preservation for all types of records, ledgers, vouchers, registers, letters, papers, and so on.

Most banks have been open to the computerized world as a result of computerization and the implementation of computerized data maintenance and, in certain cases, computer-generated vouchers. A few have also begun the process of developing their own Electronic Records Maintenance Policy. The Indian Banks' Association took the lead in publishing a book on Banks' e-Records Maintenance Policy, which can be used as a model for use and implementation in banks based on their technical setup. As a result, banks should ensure that, if not already done, e-records maintenance policy with information on e-records, their existence, upkeep, technical specifications, off-site backup, retrieval systems, access control, and access rights initiatives is in effect.

On the legal compliance side, particularly after the April 2011 Rules on Reasonable Security Practices and Procedures as part of ITAA 2008 Section 43A, banks should work hard to demonstrate that they have all of the necessary security measures in place, such as ISO 27001 compliance, and that e-records are kept up to date. Furthermore, the certificate required as an annexure to e-evidences under the BBE Act stresses the importance of maintaining e-records in a proper manner, including ensuring proper backup, preventing

tamper ability, and always ensuring confidentiality, honesty, availability, and non-repudiation.

This strategy should not be confused with the Data Warehousing plans or the Information Technology Business Continuity and Disaster Recovery Plan or Policy. All three regulations (BCDRP, DWH, and E-records Maintenance Policy) are distinct in that they serve different functions, employ different technologies, and may be subject to different managerial administrative controls.

CHAPTER 4

JUDICIAL APPROACH IN CURBING THE CYBER CRIME

The internet is a global phenomenon. India, as a formidable part of the world, experienced a seismic change in the technological landscape when the Information Technology waves swept through the region, necessitating the establishment of an Information Technology ministry in the country in 1999. Clearly, the knowledge society provides humans with a wide range of possibilities and opportunities for identifying, evaluating, and exchanging information for the good of people all over the world. Information technology creates a modern working climate, work culture, market connections, and trading networks. It enables information and knowledge-based work to be carried out from any location. It has the potential to change and revolutionize the world. Because of the inherent lack of spatiality and temporality in cyberspace, new types of ecommerce have emerged. Cybercrime is quickly becoming a threat to national and economic security. Many industries, institutions, and public and private sector organizations (especially those involved in critical infrastructure) are vulnerable. Some organisations, on the other hand, have described organized cyber-criminal networks as their greatest cyber security threat, and some are prepared to protect against such threats. Increased opportunities for productivity, production, and global connectivity drew in an influx of new users. The internet's dependability and availability are important organizational considerations. Spamming, spoofing, and other activities that challenge these attributes have serious consequences for the user community. Lawyers and legal advisors' job is also included in the developments. Given the importance of this important sector and its prominent position in the judicial system, there has been an increasing interest in regulating the legal profession in what appears to be a serious step towards advancing the profession.

As cyber-crime has spread around the globe at an unprecedented pace, those in the criminal justice community have lacked appropriate and up-to-date information about the pedestrian reality of modern cyber-crime. The popular media has portrayed cyber-crime as a lone hacker breaking through almost impenetrable security barriers to gain access to valuable secret data. These types of crimes are uncommon, but cybercrime is all too common. The increasing importance of information technology can be seen in the fact that, for the first time in India, a Delhi-based businessman has created a digital will of the confidential information stored in his e-mail account. The idea of digital will is a foreign one that is gaining traction in

India as well. The performance of the nation's legislative, judicial, and executive authorities is the source of its power. The judiciary's function is to promote justice and equality through the proper application of laws and regulations, ensuring that everyone gets their fair share. The legislature and judiciary are critical organs in any country's success in establishing successful foreign relations, attracting investment, and enacting adequate legislation. A fair and modern judicial system is required to gain the confidence of the international community and to facilitate concerted action by various entities in order to achieve the desired outcome. Because of the emergence of cyberspace alongside the old world in the last century, society requires some degree of order and consistency in order to operate in a fair and orderly manner. For a long time, safety and security has been merely a question of defense against threats from the physical world. Better legislative responses are expected in this conventional offline environment. In this chapter, an attempt is made to address the national laws that have been passed in India to tackle cybercrime.

Since cybercrime is an intangible crime, it does not necessitate physical violence or the involvement of the accused at the crime scene. Under these conditions, the conventional adversarial system of prosecution will be unable to achieve the goals of justice in cybercrime cases. In *State of Punjab and Others v. M/S Amritsar Beverages Ltd. and Others*⁷⁹, the Supreme Court of India noted that Internet and other information technology have carried with them problems that were not foreseen by law. It also didn't account for the challenges that officers could encounter if they don't have the necessary scientific knowledge or insight to deal with new situations. Various new trends leading to various types of crimes that our Legislature had not anticipated came into sharp focus right away. While the Information Technology Act of 2000 was revised to include different forms of cybercrimes and punishments for them, it does not address all of the issues that officers enforcing the Act face. Above all, in the age of cybercrime, the Indian judiciary has played a critical role. Since India's Supreme Court has been the final arbiter of laws for decades. The judicial and law enforcement authorities are well aware that the resources available to investigate and prosecute crimes and terrorist acts conducted against or by computers or computer networks are almost entirely global in nature at the moment. The judiciary's most important duty is to interpret laws in order to determine the legislature's true meaning, which is reflected in the language used in the legislation. It is stated that the court does not legislate but only interprets the laws that already exist. In the case of *Institute of Chartered Accountants of India v. Price*

⁷⁹ *State of Punjab & Ors v. M/S Amritsar Beverages Ltd. & Ors*, Appeal (Civil) 3419 of 2006.

Waterhouse⁸⁰, the Supreme Court ruled that a law is a legislative edict. The terminology used in a statute is a determining factor in determining legislative intent. The symbols that are used are the words and phrases that stimulate mental connections to referents. That is why the primary goal of reading legislation is to determine the true meaning of the legislators who enacted them.

In the case of *Grid Corporation of Orissa Ltd. v. AES Corporation*⁸¹, the Indian judiciary is playing an important role in dealing with such crimes by practicing their technical temperament. When an efficient consultation can be accomplished by resorting to electronic media and remote conferencing, it is not mandatory for the two persons needed to act in consultation with each other to sit together at one place unless it is a necessity of law or of the ruling contract between the parties, the Hon'ble Supreme Court held in this case. As a result of the advent of modern technology, the Hon'ble Supreme Court, in *State of Maharashtra v. Dr. Praful B. Desai*⁸², allowed video conferencing, stating that it is an advancement in science and technology that allows one to hear, see, and speak with someone who is far away as though they were right in front of them. In the cases of *Amitabh Bagchi v. Ena Bagchi*⁸³ and *Bodala Murali Krishan v. Smt. Bodala Prathima*⁸⁴, similar decisions were reached. In *Ponds India Ltd. v. Commissioner of Trade Tax, Lucknow*⁸⁵, the Supreme Court also accepted the idea of updating construction in order to shift towards a fast-changing technology-based society, holding that while Wikipedia is not an authentic source, it can be used to gather information. While delivering the judgment in *Mohammed Ajmal Mohammad Amir Kasab v. State of Maharashtra*⁸⁶, the court praised the electronic evidence. CCTV video, memory cards, mobile devices, data storage devices, intercepted messages over VoIP, IP addresses, and other evidence were all appreciated by the court.

In *Common Cause v. Union of India*⁸⁷, a registered society challenged the constitutional validity of Articles 66A, 69A, and 80 of the Information Technology Act by filing a writ petition under Article 32 of the Indian Constitution for the protection of Fundamental Rights under Articles 14, 19, and 21 of the Indian Constitution. In this case, it is

⁸⁰ *Institute of Chartered Accountants of India v. Price Waterhouse*, Special Leave Petition Arises from Civil Writ No. 676 of 1994.

⁸¹ *Grid Corporation of Orissa Ltd. v. AES Corporation & Ors* (2003) 1 CALLT 50 SC.

⁸² *State of Maharashtra v. Dr. Praful B. Desai*, Appeal (Crl.) 476 & 477 of 2003.

⁸³ *Amitabh Bagchi v. Ena Bagchi*, A.I.R. 2005 Cal. 11.

⁸⁴ *Bodala Murali Krishan v. Smt. Bodala Prathima*, A.I.R. 2007 AP 43.

⁸⁵ *Ponds India Ltd. v. Commissioner of Trade Tax, Lucknow*, Civil Appeal No. 3644 of 2008.

⁸⁶ *Mohammed Ajmal Mohammad Amir Kasab v. State of Maharashtra*, Appeal (Crl.) Nos. 1899-1900 of 2011.

⁸⁷ *Common Cause v. Union of India*, Writ Petition (Crl.) No. 97 of 2013.

argued that the restrictions imposed by Section 66A of the IT Act violate Article 14 because they limit free online expression, as well as Article 19 because the restrictions on speech that causes mere annoyance often go beyond the scope of appropriate restrictions set out in Article 19(2) of the Indian Constitution. It is also argued that the words grossly offensive, threat, and annoyance used in Section 66A are ambiguous, subjective, and constitutionally undefined. It is also argued that section 69A of the IT Act violates Articles 14, 19, and 21 of the Indian Constitution because it does not have a redressal mechanism after the blocking of an entity's online records, nor any provisions for unblocking them, and fails to meet constitutional safeguards of natural justice. Similarly, section 80 of the Act is in violation of Articles 14, 19, and 21 of the Indian Constitution since it gives police officers broad powers to apprehend anybody suspected of committing a crime under the Act without a warrant.

The first case in India was *Yahoo, Inc. v. Akash Arora*⁸⁸, in which an Indian court handed down a decision on domain names. Yahoo Inc. filed a lawsuit against the defendants, seeking a permanent injunction prohibiting them and their associates, servants, and agents from conducting any business on the internet under the domain name 'Yahooindia.com' or any other domain name that is similar to the plaintiff's trademark 'Yahoo!' Over the course of the lawsuit, the plaintiff filed an application for a provisional restraining order against the defendants. In this case, the Court issued an ad hoc injunction prohibiting the defendants from engaging in any internet company using the trademark/domain name Yahooindia.com or any other trademark/domain name that is similar to the plaintiff's trademark Yahoo!.

The Indian judiciary is playing a critical role in dealing with cybercrimes such as sending offensive messages via communication services, among other things. In the first cyber case, *State v. Ts. Balan and Aneesh Balan*, the Additional District Court and Sessions Court upheld a lower court verdict in 2006 and convicted a Pentecostal priest and his son for morphed images and e-mailed to victims from fake IDs with captions under section 67 of the Information Technology Act, 2000.

The government of Kerala had released a notification declaring an e-government app named 'FRIENDS,' which was created by the petitioner under a contract, as a protected framework in the case of *B.N. Firos v. State of Kerala*⁸⁹. The complainant filed a writ petition, alleging that section 70 of the Information Technology Act and the notice was illegal

⁸⁸ *Yahoo, Inc. v. Akash Arora & Anr*, 1999 IIAD Delhi 229.

⁸⁹ *B.N. Firos v. State of Kerala*, Civil Appeal No. 79 of 2008.

and in violation of the copyright act. A notice under section 70 of the Information Technology Act is deemed to be a copyright declaration under section 17 (d) of the Copyright Act, 1957. The court went on to say that only if a computer resource amounted to a government work under the copyright act could it be declared a protected system under the Information Technology Act.

Section 66A of Information Technology Act, 2000 held unconstitutional: In the wake of a series of arrests made under Section 66A of the Information Technology Act, 2000, *Shreya Singhal v. Union of India*⁹⁰ is a case where a writ petition was filed in the public interest under Article 32 of the Indian Constitution, arguing that Section 66A is too broad, vague, and unconstitutional to be judged on objective standards. The words offensive, menacing, nuisance, threat, obstruction, and insult have not been specified in the Information Technology Act, General Clauses Act, or any other legislation, it was further argued. The impossibility of framing a meaning with mathematical precision does not excuse the use of ambiguous terms, according to the ruling in *A. K. Roy v. Union of India*⁹¹. In the case at hand, a clause of the National Security Act was found to be in violation of the Fundamental Right to Life and Personal Liberty guaranteed by Article 21 of the Constitution (due to its potential for willful abuse). Citing the arrests made under Section 66A, the petitioner claims that the Section's broad legislative language discourages people from exercising their constitutionally protected right to free speech for fear of frivolous prosecution (the chilling effect), which violates Article 19(1)(a) of the Constitution's guarantee of freedom of speech and expression. Furthermore, regardless of whether section 66A passes the reasonableness test set forth in Article 19(2), it violates Articles 14 (Right to Equality) and 21 of the Constitution. In *Shreya Singhal and others v. Union of India*⁹², the Hon'ble SC ruled section 66A unconstitutional in its entirety and anti-freedom of speech and expression, and struck it down. Police in several states have used this section to falsely prosecute people for making critical remarks on social and political issues on social media platforms. Many people have been arrested as a result of this section for falsely sharing offensive material on the internet.

Furthermore, in *S. Khushboo v. Kanniammal*⁹³, the Supreme Court stated that when cases involving the constitutional right to freedom of speech and expression, Magistrates must use their legislative powers to guide an investigation into the allegations before taking

⁹⁰ *Shreya Singhal v. Union of India*, A.I.R. 2015 S.C. 1523.

⁹¹ *A. K. Roy v. Union of India*, A.I.R. 1982 S.C.710

⁹² *Supra* note 89.

⁹³ *S. Khushboo v. Kanniammal* (2010) 4 SCALE 467.

cognizance of the alleged offence. Since the petitioner requests that Section 66A of the Information Technology Act be declared unconstitutional and that the Court issue a directive that offences concerning freedom of speech and expression be regarded as non-cognizable.

A writ petition was filed in the public interest under Article 32 of the Indian Constitution in *Rajeev Chandrashekhar v. Union of India*⁹⁴ and *Common Cause v. Union of India*, challenging section 66A of the Information Technology Act, 2000 and Rules 3(2), 3(3), 3(4), and 3(7) of the Information Technology (Intermediaries Guidelines) Rules, 2011 as unconstitutional. In this case, the Petitioner, a sitting Member of Parliament, claims that Section 66A comprises many undefined, ambiguous, and potentially troublesome words/terms. This imposes legislative limitations on the exercise of internet freedom that go well beyond the Constitutional parameters of reasonable restrictions enshrined in Article 19(2). Rule 3(2) of the Intermediaries Guidelines Rules specifies the different types of information that cannot be carried on a computer system, which is arbitrary and overly broad, and therefore violates Article 14 by being arbitrary and overly broad.

The Bank NSP Case: In this instance, a bank management trainee was engaged to be married. Using the company's machines, the couple exchanged several emails. They had broken up their marriage after some time, and the young lady set up some fake email accounts, such as Indian bar associations, and sent emails to the boy's foreign clients. She did this on the bank's machine. The boy's business suffered significant losses as a result of the bank's actions, and he brought the bank to court. The bank was kept responsible for emails sent via the bank's system.

Bazee.com Case:⁹⁵ The accused is the CEO of Baaze.com, a company that promotes the selling of any property in exchange for a fee and also makes money from advertisements on its website. In this case, the State's counsel has claimed that the accused was negligent, on pain of culpability, in failing to avoid payment by banking networks after learning of the transaction's unlawful existence. It has been adamantly argued that denying bail would have a negative effect on e-commerce, with India potentially losing out. These are not considerations in which India could come out on the losing end. These are not factors that would influence the Court's decision on whether to grant or deny bail. Mr. Jaitley, counsel for the petitioner, has stated that a person who publishes or transmits any material that is lascivious or appeals

⁹⁴ *Rajeev Chandrashekhar v. Union of India*, WP (Crl.) No. 23 of 2013.

⁹⁵ *Avinash Bajaj v. State (NCT) of Delhi*, (2005) 3 Comp LJ 364 (Del.).

to the prurient interest commits an offence under Section 67 of the Information Technology Act, 2000. Sections 292 and 294 of the Indian Penal Code, which deal with the sale, letting on hire, distribution, and public exhibition of obscene matter, have also been listed. He has stressed that the clause does not include the act of causing the transmission, as opposed to the act of publishing obscene content. Prima facie, no publication by the accused, either directly or indirectly, has been identified based on the facts gathered to date. The real pornographic recording/clip is not viewable on Basse.com's portal.

The accused was found to have voluntarily engaged in the investigations, and Counsel for the State offered no evidence to the contrary. Because of the nature of the suspected crime, the evidence has already crystallized and can be tamper-proof. Despite the fact that the accused is no longer an Indian citizen, he is of Indian descent and has family ties to our nation. It is impossible to claim that a foreign national is not eligible for bail. The accused is granted bail in the amount of Rs. 1,00,000/- each, subject to the satisfaction of the concerned Court/ Metropolitan Magistrate/Duty Magistrate. The Accused cannot leave India's territories without the permission of the Court, and he must surrender his passport to the Magistrate for this reason. The fact that he was granted bail implies that he would cooperate and engage in the investigation. The Bail Application has been dismissed.

Parliament Attack Case: The Bureau of Police Research and Development in Hyderabad handled the case of the Parliament Attack. The terrorist who attacked the Parliament was found with a laptop. The laptop taken from the two attackers who were gunned down on the 13th of December 2001 when the Parliament was under attack was sent to the BPRD's Computer Forensics Division. The laptop contained several proofs that affirmed the two terrorists' motives, including a Ministry of Home sticker that they had made on the laptop and affixed to their ambassador car to gain access to Parliament House, as well as a fake ID card with a Government of India emblem and seal that one of the two terrorists was carrying. The emblems (of the three lions) were meticulously scanned, and the seal was handcrafted, complete with a Jammu and Kashmir residential address. However, close examination revealed that everything was forged and created on the laptop.

Andhra Pradesh Tax Case: The owner of a plastics company in Andhra Pradesh was arrested, and the Vigilance Department seized Rs. 22 from his home. They needed him to provide proof of the unaccounted cash. The suspect submitted 6,000 vouchers to prove the validity of his trade; however, a close examination of the vouchers and the contents of his

computers revealed that each one was generated after the raids. It was hidden that the suspect was running five enterprises under the guise of one, and that he was using false and computerized coupons to display sales reports and avoid paying taxes. As a result, when officials from the department obtained computers used by the accused individual, the questionable tactics of the state businessman were revealed.

Sony.Samandh.Com Case: It all started when Sony India Private Ltd, which operates the www.sony-samandh.com website that targets non-resident Indians, filed a complaint. NRIs may use the website to send Sony items to friends and relatives in India after paying for them online. The organization guarantees that the goods will be delivered to the intended recipients. In May 2002, someone using the name Barbara Campa logged into the website and placed an order for a Sony Color Television and a cordless phone. She demanded that the items be sent to Arif Azim in Noida and gave her credit card number for payment. The credit card company cleared the invoice and processed the transaction. The products were shipped to Arif Azim after the company completed the required due diligence and inspection procedures. The business took digital photographs of Arif Azim accepting the order at the time of delivery. The transaction was completed at that point, but after one and a half months, the credit card company told the company that the payment was illegal because the real owner had denied making it.

The company filed an online cheating complaint with the Central Bureau of Investigation, which opened an investigation under Indian Penal Code Sections 418, 419, and 420. Arif Azim was arrested after the matter was investigated. Arif Azim obtained the credit card number of an American national while working at a call center in Noida, which he misused on the company's website, according to investigations. The color television and cordless phone were recovered by the CBI. The CBI had evidence to support their argument in this case, but the accused confessed his guilt. Arif Azim was found guilty under Sections 418, 419, and 420 of the Indian Penal Code, marking the first time a cybercrime has been found guilty. The court, on the other hand, believed that since the accused was a young boy of 24 years old and a first-time offender, a lenient approach was needed. As a result, the accused was sentenced to a year of probation. The decision has enormous ramifications for the entire nation. Apart from being the first cybercrime conviction, it has shown that the Indian Penal Code can be successfully extended to such types of cybercrime that are not protected by the Information Technology Act 2000. Second, a decision like this sends a strong message to all that the law cannot be manipulated.

SMC Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatra:⁹⁶ In India's first case of cyber defamation, a Delhi court took jurisdiction over a case in which a company's image was being slandered via emails and issued a significant ex-parte injunction. In this case, the defendant Jogesh Kwatra, who worked for the plaintiff firm, began sending insulting, defamatory, pornographic, lewd, disgusting, and abusive emails to his employers as well as to various subsidiaries of the said company around the world in order to defame the company and its Managing Director Mr. R K Malhotra. The plaintiff filed a lawsuit seeking a permanent injunction to prevent the defendant from sending offensive emails to the plaintiff. It was argued on behalf of the plaintiffs that the defendant's emails were clearly pornographic, lewd, violent, threatening, degrading, and defamatory. Counsel went on to say that the aim of sending the emails was to smear the plaintiffs' good name in India and the world. He went on to say that the defendant's actions in sending the emails had infringed on the plaintiffs' civil rights. Furthermore, the defendant has a legal obligation not to send the above letters. It's worth noting that the plaintiff corporation terminated the defendant's services after discovering the employee could have been sending threatening emails. After hearing the plaintiff's counsel's extensive arguments, the Hon'ble Judge of the Delhi High Court issued an ex-parte ad interim injunction, stating that the plaintiff had formed a prima facie case. As a result, the Delhi High Court barred the defendant from sending defamatory, pornographic, vulgar, degrading, or abusive emails to the plaintiffs or its sister subsidiaries around the world, including their Managing Directors and Sales and Marketing divisions. Furthermore, the defendant was barred from writing, distributing, or causing to be released any material that is negative, defamatory, or abusive of the plaintiffs, both in the real world and in cyberspace. This order by the Delhi High Court is significant because it is the first time an Indian court has taken jurisdiction in a case involving cyber defamation and issued an ex-parte injunction prohibiting the defendant from defaming the plaintiffs by sending insulting, defamatory, threatening, or obscene emails to the plaintiffs or their subsidiaries.

NASSCOM v. Ajay Sood & Ors:⁹⁷ The Delhi High Court ruled phishing on the internet to be illegal in the case of National Association of Software and Service Companies vs Ajay Sood & Others⁹⁸, delivered in March 2005, resulting in an injunction and damages recovery. In order to set a precedent in India, the court described phishing as a type of internet fraud in which an individual impersonates a legitimate organization, such as a bank

⁹⁶ SMC Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatra, RFA 268 OF 2014.

⁹⁷ NASSCOM v. Ajay Sood & Ors, 119 (2005) DLT 596

⁹⁸ *Id.*

or an insurance firm, in order to obtain personal data from a customer, such as access codes, passwords, and so on. Personal data obtained by misrepresenting the identity of the rightful party is often used for the benefit of the collecting party. As an example, the court noted that traditional phishing scams involve people impersonating online banks and siphoning money from e-banking accounts after duping customers into handing over sensitive banking information. Despite the fact that there is no clear legislation in India that criminalizes phishing, the Delhi High Court declared it to be an illegal act, describing it as a misrepresentation made in the course of trade leading to uncertainty as to the source and origin of the e-mail causing immense harm not only to the recipient but also to the individual whose name, identity, or password is misused. The court ruled that phishing is a form of impersonation that tarnishes the plaintiff's image. The National Association of Software and Service Companies (Nasscom), India's premier software association, was the plaintiff in this case. The defendants ran a placement firm that specialized in headhunting and recruitment. The defendants wrote and sent e-mails to third parties in the name of Nasscom in order to collect personal data that they could use for head-hunting purposes. The plaintiff's trademark rights were recognized by the high court, which issued an ex-parte ad-interim injunction prohibiting the defendants from using the trade name or any other name that is confusingly similar to Nasscom. The defendants were also barred from claiming to be friends or members of Nasscom, according to the court. A commission was named by the court to execute a search warrant at the defendants' residence. The local commissioner appointed by the court took possession of two hard disks from the machines from which the defendants sent false e-mails to different parties. The incriminating e-mails were then extracted from the hard drives and submitted in court as evidence. As the case progressed, it became apparent that the defendants in whose names the offending e-mails were sent were fake identities created by an employee on the defendants' orders in order to escape detection and legal action. The fictional names were removed from the list of defendants in the case after this fraudulent act was discovered. Following that, the defendants confessed to their wrongful actions, and the parties reached an agreement in the suit proceedings by recording a settlement. According to the terms of the settlement, the defendants decided to pay the plaintiff Rs1.6 million in damages for infringement of the plaintiff's trademark rights. The hard disks confiscated from the defendants' premises were also ordered to be handed over to the complainant, who would be the rightful owner of the hard disks. This case accomplishes the following objectives: It clarifies the misconception that there is no damages culture in India for violations of IP rights; It reaffirms IP owners' faith in the Indian judicial system's ability and willingness to

protect intangible property rights and sends a strong message to IP owners that they can do business in India even in the absence of specific legislation; It clarifies the misconception that there is no damages culture in India for violations of IP rights; It reaffirms IP owners' faith in the Indian judicial system.

Dilip Kumar Tulsidas v. UOI:⁹⁹ The petitioner in Dilip Kumar Tulsidas v. Union of India has also asked the court to order the respondents to conduct widespread public awareness campaigns about cyber-crime, which is punishable under the Information Technology Act and other laws. There are no procedural protections in place in the current cybercrime investigation scheme. There have also been a number of cases where the police and cooperating private companies have shown great negligence against innocent people, and the forensic procedures used to deal with complex cyber-crimes are inadequate.

People's Union for Civil Liberties v. Union of India:¹⁰⁰ Despite the Supreme Court issuing a similar notice in Shreya Singhal v. U.O.I shortly before this, a writ petition was filed in the public interest under Article 32 of the Constitution of India regarding the misuse of the Rules framed under the IT Act throughout the country in People's Union for Civil Liberties v. Union of India. Articles 14, 19, and 21 of the Information Technology (Intermediaries Guidelines) Rules, 2011, which provide for legal determinations and efficient censorship by private on-line service providers, are ambiguous and undefined categories. The Information Technology (Procedure and Safeguards for Blocking for Public Access to Information) Rules, 2009, which provide that the blocking process is completely secret, fail to meet constitutional safeguards of natural justice under Articles 19 and 21, and the unreasonably restrictive procedure for banning websites also fails to meet procedural natural justice standards for book bans.

Syed Asifuddin & Ors v. State of Andhra Pradesh & Ors:¹⁰¹ Under the Dhirubhai Ambani Pioneer Scheme, the subscriber purchased a Reliance phone and Reliance mobile services at the same time. The customer was enticed by better tariff plans offered by other service providers and desired to switch to them. The Electronic Serial Number (hereinafter referred to as ESN) was hacked by the petitioners (TATA Indicom employees). Reliance handsets' Mobile Identification Numbers (MIN) was irreversibly linked to ESN, and reprogramming ESN made the system legitimate only by Petitioner's service provider, not by

⁹⁹ Dilip Kumar Tulsidas v. Union of India, WP (Crl.) No. 97 of 2013

¹⁰⁰ People's Union for Civil Liberties v. Union of India (2013) 10 SCC 1.

¹⁰¹ Syed Asifuddin & Ors v. State of Andhra Pradesh & Ors, 2005 CriLJ 4314.

Reliance Infocomm. The Court was asked whether a telephone handset is a computer under Section 2(1)(i) of the IT Act, and whether manipulating ESN programmed into a cell handset constitutes source code modification under Section 65 of the IT Act.

According to the court, a computer is defined as any electronic, magnetic, optical, or other high-speed data processing device or system that performs logical, arithmetic, or memory functions by manipulating electronic, magnetic, or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities that are a part of it. As a result, a telephone handset falls within the definition of machine as specified in Section 2(1)(i) of the IT Act.

Pune Citibank Mphasis Call Center Fraud: In 2005, \$ 3,50,000 was fraudulently transferred from four Citibank accounts in the United States to a few fake accounts via the internet. The employees earned the customers' confidence and secured their PINs under the expectation that they would be able to assist them in dealing with challenging circumstances. Instead of decoding encrypted software or breaching firewalls, they were looking for flaws in the Mphasis framework. The defendants in this case are Mphasis call center ex-employees, according to the court. Any time an employee enters or exits, they are reviewed. As a result, it's obvious that the workers had the numbers memorized. SWIFT, or the Society for Worldwide Interbank Financial Telecommunication, was used to move the money. Unauthorized access to the customers' electronic accounts was used to commit the fraud. As a result, this case is classified as a "cyber-crime." The IT Act is broad enough to include all types of offenses, and any IPC offense involving the use of electronic records may be prosecuted on the same level as crimes involving written documents. Because of the type of unauthorized access that is involved in committing transactions, the court held that section 43(a) of the IT Act, 2000 is valid. The accused were also charged under sections 66 and 420 of the Information Technology Act, 2000, as well as sections 465, 467, and 471 of the Indian Penal Code, 1860.

Christian Louboutin SAS v. Nakul Bajaj & Ors:¹⁰² The Complainant, a luxury shoe maker, filed a lawsuit seeking an injunction against www.darveys.com, an e-commerce site, for engaging in trademark infringement in the sale of counterfeit products. The Court had to decide if the defendant's use of the plaintiff's name, logos, and image was covered under Section 79 of the Information Technology Act. The defendant is more than an agent,

¹⁰² Christian Louboutin SAS v. Nakul Bajaj & Ors (2018) 253 DLT 728.

according to the Court, because the website has complete control over the goods offered through its portal. It identifies and encourages third-party vendors to sell their wares. The Court also stated that an e-commerce platform's active involvement would exclude it from the rights granted to intermediaries under Section 79 of the IT Act.

State of Tamil Nadu v. Suhas Katti:¹⁰³ The accused was a close associate of the victim's family. The accused wanted to marry the survivor, but she declined and married someone else instead. However, the marriage ended in divorce. That's why the accused tried to reach the victim again, but she turned him down once more. After that, the accused began harassing her online by sending her insulting and defamatory messages via Yahoo Messenger. In addition, the accused forwarded emails received in a fictitious account he created in the victim's name. The victim received anonymous calls as a result of the uploading of messages. The calls were made under the impression that the victim was looking for sex work. The survivor had had enough of the threats and lodged a complaint against him. The accused was apprehended and stated unequivocally that he did not commit the crime.

The offending emails and texts, according to the defense attorney, were sent by her ex-husband or someone else. He also said that the victim wanted to marry the accused and that after being refused, the victim attempted to frame the accused with false accusations.

On November 5, 2004, a Metropolitan Magistrate in Egmore handed down a decision in this case. The victim presented evidence in the form of the harasser's IP address matching that of the perpetrator, and the owner of the cybercafé, who was an eyewitness, testified against the accused. The accused was found guilty of violating Sections 469, 509 IPC, and Section 67 of the Information Technology Act, 2000 by the Magistrate.

“According to Section 469 of the Indian Penal Code, whoever commits forgery (intentionally forging a document or electronic record) with the intent to damage the reputation of another party, or knowing that it is likely to be used for that reason, is punishable by imprisonment of any description for a term up to three years, as well as a fine.”

“According to Section 509 of the Indian Penal Code, whoever utters any word, makes any sound or gesture, or exhibits any object with the intent that such word, sound, gesture, or

¹⁰³ State of Tamil Nadu v. Suhas Katti, CC No. 4680 of 2004.

object be heard, or that such gesture or object be seen, by such woman, or intrudes upon her privacy, shall be punished.”

“According to Section 67 of the Information Technology Act of 2000, anyone who publishes, transmits, or causes to be published or transmitted in electronic form any content that is lascivious, appeals to the prurient interest, or attempts to deprave and corrupt people is guilty of a crime.”¹⁰⁴

He was sentenced to two years of rigorous imprisonment and a fine of Rs.500/- under section 469 IPC, one year of plain imprisonment and a fine of Rs.500/- under section 509 IPC, and two years of imprisonment and a fine of Rs.4,000 under section 67 of the IT Act 2000.¹⁰⁵

¹⁰⁴ Riddhika Vartak, *Case Analysis: State of Tamil Nadu v. Suhas Katti*, Legal Acharya (Nov 22, 2020), <https://legalacharya.com/caseanalysis/case-analysis-state-of-tamil-nadu-v-s-suhas-katti-2004/>.

¹⁰⁵ *Id.*

CHAPTER 5

CONCLUSION & SUGGESTIONS

5.1 Conclusion:

Since the 1990s, cyberspace has evolved at such a rapid and massive pace that codes of ethics, common sense of justice, and criminal laws have failed to keep up. Cybercrime has had a brief but eventful past, to say the least. There are several points of view on the real nature of this modern type of crime. Some argue that cybercrime has existed since the advent of the computer with the invention of the first abacus and people have used calculating machines for improper purposes. Actually, the history of cybercrime began with hackers attempting to break into computer networks solely for the thrill of gaining access to high-security networks or obtaining confidential or protected information or other secret for personal gain or revenge. In the field of criminology, it has been said that a crime will occur when and only when the opportunity arises. Previously, we just knew of typical forms of crimes such as murder, rape, stealing, extortion, robbery, and dacoity. However, with the advent in science and technology, such as computers and internet facilities, new forms of crimes have emerged, such as hacking, cyber pornography, and cyber defamation. The word cybercrime is misleading. There is no distinction between identifying a crime in the cyber world and the real world because cyber-crimes are simply real-world crimes perpetrated through the medium of a machine. Just the crime medium is different. There are no cyber-borders between countries in these international or transnational situations. Computer crime, cybercrime, e-crime, hi-tech crime, or internet crime are all synonyms for illegal activity that takes place in cyberspace and involves the use of a computer or network as a source, target, or weapon. In the United States and the United Kingdom, there is no legal term. Surprisingly, the word cyber-crime or cyber offence is not specified in India, nor is it included in the Information Technology Act of 2000. Even after being amended by the Information Technology (Amendment) Act, 2008, the Indian Penal Code, 1860, does not use the word cyber-crime at any stage. Cybercrime is inherently silent, and it can be carried out in the privacy of one's own home without the need for the perpetrator to be physically present in front of the victim or for any eye witnesses. There are no signs of physical abuse or cries of distress during the commission of such offenses since a cyber-criminal commits the crime quietly and without fear of being caught red-handed. These crimes can be carried out with a single click of the mouse and without the victim's knowledge. In the majority of these types

of crimes, the victim has no idea what has happened to him, who has done it to him, or when it was done. Because of a lack of successful national and international efforts to detect cyber criminals, it is extremely difficult to do so.

The growth of computer networks has resulted in cybercrime. The Internet has been all-pervasive and omnipresent in the new millennium. It has also brought with it new challenges that mankind has never faced before. In certain ways, the Internet is similar to the "high seas," where no one owns but which is used by citizens of all nationalities. The word 'cybercrime' refers to a wide range of illegal activities that take place in cyberspace through global communication and knowledge through the internet. It is an unavoidable evil that stems from mankind's the reliance on computers in modern existence, with the explanation being that computers, while being high-tech machines, are extremely fragile. As a result, any crime or illegal activity that involves the use of a device is considered a cybercrime. As a result, "cybercrime" has been described as "an unlawful act in which the computer is used as a weapon, a target, or both."

According to the preceding analysis, cybercrimes are malicious activities carried out in cyberspace that can harm an individual, property, or even the state or society as a whole. Many cybercrimes are committed by criminals all over the world who use computer technology to commit their crimes. Since cybercrimes are so dissimilar from traditional crimes, law enforcement authorities are finding it difficult to combat them using current infrastructure due to a lack of sufficient knowledge of computer operating systems. This is the primary explanation why the justice system is being tested by this relatively new type of crime. The invention of the internet has aggravated the issue even more. The threat of cybercrime is not limited to one or two countries; rather, the entire world is confronted with this massive problem as a technological scorn. India is not immune to the threat posed by computers. The Information Technology Act of 2000, which went into effect on October 17, 2000, was passed by Parliament as a measure to deter and regulate internet crimes. Offenses relating to cyberspace are categorically described in the Act, including tampering with computer source documents, hacking with computer systems, violation of confidentiality and privacy, and so on. It's not because there was no statute in place to deal with these offenses before this legislation. The Indian Penal Code of 1860 also had provisions to deter and regulate cybercrime, but they were found to be insufficient to deal with all types of cybercrime. The simple explanation is that at the time the Indian Penal Code was enforced, no one had heard of a machine or the internet.

It is hardly necessary to point out that science and technology have spread their tentacles across national borders, whilst the law continues to struggle to identify and redefine the parameters for cybercrime regulation. Following a similar path, cyber law, specifically the Information Technology Act, focuses on the prevention and control of cybercrime within the country's territorial jurisdiction, despite the fact that cybercrime is a global phenomenon that knows no borders. There have been many debates on how cybercrime should be classified. However, the viewpoints vary from one another. First, which practices on the internet should be criminalized and classified as cyber-crimes, and second, all forms of cyber-crimes include both the machine and the individual using it as victims, since most people in today's technical world are unaware of which types of crimes fall under the category of cyber-crime. In addition, the United States has not given any formal classification of cybercrime. The Computer Misuse Act of 1990 in the United Kingdom categorizes cybercrime into three sections, while the Information Technology Act of 2000 in India does. Owing to a lack of adequate and uniform classifications of such crimes, as well as effective counter-measures, these crimes are becoming more common by the day. The IT Act is regarded as major cyber legislation in India because it is the only law in the field of information technology that devotes itself entirely to electronic situations, such as e-transactions, e-commerce, e-governance, and so on, with cyber-crimes gradually protected as well. The Indian Penal Code, 1860; the Indian Evidence Act, 1872; the Bankers Book Evidence Act, 1891; and the Reserve Bank of India Act, 1934 are all amended by the Information Technology Act. Owing to some inconsistencies, it was revised in 2008. However, the issue of cybercrime persists, and it is discovered that the statute's application is based more on paper than on execution, since attorneys, police officers, prosecutors, and judges are unable to comprehend its extremely technical terminology. The Information Technology Act of 2000 was passed to encourage e-commerce, but it has been found to be ineffective in dealing with a number of other emerging cyber-crimes. These crimes are on the rise as a result of a lack of robust cyber legislation and effective regulation to fight cybercrime. In cases where hackers are outside India's territorial borders notwithstanding the provisions of section 1 (2) and section 75 of the IT Act, 2000, it is determined that Section 66 of the IT Act would not be an adequate remedy and that the offence is bailable in nature, allowing for immediate release on bail. The 50th Report of the Standing Committee on Information Technology in 2007-2008 on the Information Technology (Amendment) Bill, 2006, heavily criticized the amendment to Section 66 made by the Amendment Act, 2008, which replaced hacking with computer-related offenses on the grounds that it has greatly

narrowed the scope of application of the section and also creates difficulty for law enforcement. Before the new amendment, the concept of hacking had a very broad scope that included the majority of computer-related offenses and was still broad enough to encompass any newly emerging cyber-crimes.

The requirement that the act be performed with the intent to defraud or cause wrongful harm or benefit was the key source of criticism. This implies a much higher degree of mens rea than the old section 66 of the Act, which allowed a person to be found guilty only if they had mere knowledge of the risk of injury. However, an individual may no longer be held liable under section 66 if the act was performed without the intent to defraud or cause unjust harm or benefit. Section 66 A seems to have been added with the aim of protecting people's reputations and avoiding the abuse of networks. However, the language used in the section goes well beyond the fair limitations that can be placed on free speech under Article 19(2) of the Indian Constitution, potentially jeopardizing the fundamental right to free speech in social media. The essence of the offense is cognizable under section 66A, and police authorities were initially allowed to detain or prosecute without warrants based on charges brought under the section. This will lead to a slew of high-profile prosecutions of people for uploading objectionable content online, with the 'objectionable' content frequently being opposing political views. Authorities largely ignored the relief given by the Central Government in the form of an advisory in January 2013, which stated that no arrests under 66A should be made without prior approval of an officer not below the rank of Inspector General of Police. In *Shreya Singhal and others v. Union of India*, the Hon'ble Supreme Court ruled section 66 A unconstitutional and anti-freedom of speech and expression, and struck it down because this section had been widely misused by police in various states to arrest innocent people for posting critical comments about social and political problems on social networking sites. On certain grounds, the Information Technology (Intermediaries Guidelines) Rules, 2011, have also been criticized. These regulations weaken the section 79 exemptions, which exempt intermediaries from liability in certain circumstances and have been found to compel intermediaries to filter material and practice on-line censorship. Aside from these regulations, the Information Technology (Procedure and Protections for Blocking for Access to Information by the Public) Rules, 2009 provide for blocking if information is discovered to be undisclosed and does not follow constitutional safeguards of natural justice. Terrorists in society were motivated to use information technology as a weapon and as objectives in order to achieve their goals. Cyber terrorism has evolved into one of the most

dynamic national and international threats of our time, in which one nation targets another through the use of technology.

This definition is still undefined in the IT Act. International terrorists attack using websites, such as Al-Qaida's websites which have links to Osama Bin Laden's attack on India's Parliament on December 13, 2001 by creating a false gate pass from the internet, the September 11, 2001 attack on the WTO and Pentagon, the December 16, 2005 e-mail threat to attack the Indian Parliament and US consulate, and Aftab Ansari's attack on the American Information Centre in Kolkata. In India, there is very little litigation because the private sector is afraid of negative publicity if they report cybercrimes, resulting in less judicial pronouncements. The majority of cases go unreported due to a lack of public awareness and information. As a result, cyber criminals have become more interested in committing such crimes. These crimes have arisen as a result of the lack of multi-threat protection systems, technology-based programs or camps, and the failure of national and international organisations to follow foolproof computer procedures. Without a doubt, the Indian legislative and judicial systems play an important role in combating such crimes, but in some cases, the legal structure is found to be insufficient to address the challenges posed by cybercrime, which has emerged as a human rights problem. There has been a lack of judicial response to cybercrime in India, as well as inadequate legislation to deal with these types of crimes, which will be a major challenge for the Indian judicial system in the near future. It is also discovered that law enforcement actions and practices related to cybercrime investigations are never flawless. That if a law enforcement officer makes a mistake, law-abiding citizens will suffer as a result. Due to the easier availability and wider dissemination of US laws and principles around the world, the Indian judiciary can be tempted to apply the principles developed by US courts. The failure of lawmakers to keep cybercrime laws ahead of the fast-moving technical curve has long frustrated law enforcement officials. If such a situation arises, policymakers must strike a balance between conflicting interests such as individual rights to privacy and free expression, as well as the need to preserve the integrity of the world's public and private networks. It has also been discovered that, in the modern era, investigating agencies and law enforcement agents use the same methods for gathering, analyzing, and reviewing evidence when investigating cybercrimes as they do when investigating conventional crimes. Since the essence of these offenses under the IT Act is bailable and cognizable, the police will have more discretion.

This condition has arisen as a result of a lack of appropriate legislation on jurisdictional questions, cyber courts, and specialized preparation for investigating officers, prosecutors, judges, and advocates at both the national and international levels. According to Justice A.K. Ganguly, cybercrime is invading the privacy of ordinary people, which is a violation of human rights. This is a very serious threat, as it compromises privacy, he correctly said. The majority of such crimes go unreported. Today's world is ruled by information technology. It has resulted in a significant deterioration of conventional modes of government. The police and government departments are in charge of crime prevention, but the judiciary has nothing to do with it. The United States and the United Kingdom are two conventional large countries that are standing firm against the silicon onslaught. The United States has enacted the most cyber-specific legislation, followed by the United Kingdom, which, in addition to cyber regulations, has extended conventional laws to the thorny areas at the same time. However, it was discovered that UK judges were unable to apply conventional laws to modern cases, demonstrating the need for specific technology legislation. The judicial and law enforcement authorities are well aware that the resources available to investigate and prosecute crimes and terrorist acts conducted against or by computers or computer networks are almost entirely foreign in nature at the moment. As a result, the legal frameworks of these two countries have been used as reference points in nearly all studies. Though both countries have extensive legislation to deal with these offences, in some cases it is found to be inadequate, which would pose a significant challenge to the international justice system in the near future. Many attempts are currently being made to create a shared agenda for harmonizing the environment between nations in order to tackle cybercrime through international treaties, conventions, or commissions, such as the UNCITRAL Model Law. Despite the fact that both countries have legislation to fight cybercrime, many complex legal questions remain unanswered. Since there are no appropriate rules on a global level, the legal positions relating to electronic transactions and civil liability in cyberspace are still ambiguous or unclear. This is attributable to a lack of coordination between three key components: law enforcement, adjudication, and correction, which results in inefficient resource allocation and delays the justice process. Additionally, these three segments often act in a disorganized manner with little understanding of what the other segments are doing. Both cybercrime and legal concerns are global in scope.

International organizations such as the G-8 Group, OAS (Organization of American States), APEC (Asia-Pacific Economic Cooperation), and the Council of Europe have made

numerous efforts to ensure harmonization of provision in individual countries, but such an approach is found to be critical in the investigation and prosecution of attacks against computer infrastructure. Because of the existence of cybercrime, any cybercriminal can commit a crime from anywhere on the planet. It is not necessary to go to the victim's location in order to commit a crime against him. There is a lack of a universal legal structure that should be implemented internationally and supported by specialized and professionally trained law enforcement mechanisms as well as adequate public awareness. Since the internet is everywhere, committing a cybercrime by, for example, uploading content to the internet results in the illegal act being committed everywhere on the internet at the same time. As a result, defamatory comments posted on newsgroups or social media on the internet are open to anyone with an internet connection anywhere in the world. Another factor that complicates the proper prosecution of cybercrime is that of legal authority. It has been discovered that, similar to pollution control regulations, one country cannot effectively enforce laws that comprehensively solve the issue of internet crimes without the cooperation of other nations. Many countries seem to be unable to share the urgency of combating cybercrime for a variety of reasons, such as differing values on piracy or espionage, whereas major international organizations such as the OECD and the G-8 are seriously debating cooperative schemes. India has yet to sign the Cyber Crime Convention, which was opened for signatures on November 23, 2001 in Budapest with the aim of combating cyber-crime. Owing to a lack of proper cyber laws on the issue of jurisdiction and the failure to sign the extradition treaty, the issue of jurisdiction in cyberspace remains unresolved. Because a large number of cyber laws have been passed and amended in the United States, the United Kingdom, and India, there is a lack of proper implementation of existing cyber laws and awareness among public and law enforcement agencies at both the national and international levels. However, in the absence of these rules, cybercrime is on the rise.

5.2 Suggestions:

In this age of liberalization and globalization, cybercrime must be recognized as a major new phenomenon with global political, social, and economic implications. Established organized criminals can use sophisticated techniques to communicate between groups and within a community to finance and establish networks for illicit arms trafficking, money laundering, drug trafficking, pornography, and other cybercrimes thanks to the internet's global connectivity. The methods for combating these crimes can be divided into three categories: cyber laws, education, and policymaking. Many of the above methods for dealing

with cybercrime are either ineffective or ineffective. This lack of work necessitates either improving existing work or developing new paradigms for combating cyber-attacks.

Given the growing scope of computer-related crimes, adequate regulatory legal initiatives must be adopted, as well as the law enforcement apparatus, to effectively combat the issue of cybercrime. Even a brief pause in the investigation can give cyber criminals enough time to remove or erase important data in order to avoid detection, resulting in significant financial loss to the internet user or victim. Apart from that, the unusual essence of cybercrime is that the perpetrator and the victim(s) do not meet face to face, allowing offenders to carry out sophisticated criminal acts without fear of being caught or prosecuted. As a result, for successful handling of cybercrime cases, a multi-pronged approach and concerted efforts of all law enforcement functionaries are far more needed. A single cybercrime regulatory law that is widely accepted by all countries may be a feasible option for preventing and controlling cybercrime. The mechanism of crime reduction necessitates the active participation and cooperation of individuals, institutions, businesses, and the government. As a result, a sound cybercrime prevention strategy necessitates the mobilization of community interest in combating this danger. This necessitates the active participation of all those who believe that the rising occurrence of cybercrime poses a threat to society as a whole. It also encourages people who are vulnerable to cybercrime to take steps to defend themselves. They must have a sufficient understanding and comprehension of the existence and seriousness of these offenses, as well as the dangers they pose. Obviously, the media has an important role to play in informing people about the potential dangers and negative consequences of cybercrime on victims as well as the country, as well as the required safety measures to tackle this hi-tech criminality. Another indicator of cyber-crime prevention is regulatory regulation by successful legislation. It is possible to keep these crimes under control by having law enforcement authorities enforce the law effectively. Legal prevention measures can aid in the reduction of cybercrime if they receive active community support in exposing the criminals. Other recommendations for preventing and reducing cybercrime at the domestic level include:

In order to be more relevant and comprehensive in today's environment, the Information Technology Act must be updated: The Information Technology Act of 2000, as amended by the Amendment Act of 2008, states that the Act was passed with the aim of providing legal recognition for transactions carried out by electronic data interchange and other forms of e-commerce, as well as amending the Indian Penal Code, 1860, Indian

Evidence Act, 1872, and The Bankers Book of Evidence Act, 1860. This Act's goal is to identify such offenses and include punishments, rather than to eradicate illegal behavior. The problem of cybercrime persists, and it is discovered that the statute's application is based more on paper than on execution, since attorneys, police officers, prosecutors, and judges are unable to comprehend its highly technical terminology. It is necessary to take a number of appropriate steps in order to make the Information Technology Act more applicable. The IT Act of 2000 is primarily intended to encourage e-commerce, but it is ineffective in dealing with and identifying a variety of other emerging cybercrimes such as domain name theft, cybersquatting, or other fraudulent domain name registration, spamming, chat room violations, and viewing pornographic websites, among others. The Act's list of offenses is not complete, and no illustrations or explanations are given for those offenses. In the age of Global Communication Convergence and Mobile Technology, there is a need to provide a clear description of the term cybercrime and other classified crime, to provide examples of cyber-crimes for better comprehension, and to improve cybercrime penalties while keeping international and jurisdictional aspects in mind. Almost all of the offenses punishable under the Act are bailable, so it is a matter of right to be released on bail right away. Except for cyber terrorism, which carries the highest penalty under this Act, the punishment for dealing with such crimes is also very light. It is necessary to take a range of appropriate steps in order to make the Information Technology Act more applicable and comprehensive in today's environment. Despite the provisions of section 1 (2) and section 75 of the IT Act, 2000, and the nature of the crime being cognizable, section 66 of the IT Act will not be an effective recourse in cases where hackers are outside the territorial limits of India and the nature of the offence is cognizable, which led to easy release on bail as a matter of right. This provision was inserted with the aim of protecting people's reputations and preventing network abuse, and police authorities were initially allowed to arrest or prosecute without warrants based on charges brought under the section. This will lead to a slew of high-profile prosecutions of people for uploading objectionable content online, with the 'objectionable' content frequently being opposing political views. Authorities largely ignored the relief given by the Central Government in the form of an advisory in January 2013, which stated that no arrests under 66A should be made without prior approval of an officer not below the rank of Inspector General of Police. Section 66 A of the Indian Cyber Law must be amended to make it successful, compliant with the Indian Constitution's guarantee of freedom of speech and expression, and compatible with digital media, rather than being struck down as in the Shreya Singhal case. Cybercrimes punishable under section 66 E must be identified immediately, and

after an investigation, the perpetrator must be prosecuted to the full extent of the law, such that such offenders serve as a deterrent to other criminals. The word cyber terrorism is not described in any way in the IT Act. A police officer with the rank of Inspector or higher has the authority to investigate any crime committed under this Act, according to Section 78 of the Information Technology Act, as amended by the Amendment Act of 2008. It means that the victims are difficult to reach, and as a consequence, the vast majority of incidents go unreported and uninvestigated. As a result, the police rank must be reduced to even lower than that of an Inspector of Police. There is no clear provision in the Information Technology Act for identifying and punishing cyber spamming. Spamming has been the most dangerous act in the cyber world in recent years. As a result, the Anti-Spam legislation must be enacted for the safety of children. The May- SPAM Act of 2003, enacted in response to an increasing number of complaints about spam e-mails, is also the first cyber legislation in the United States to create national standards for sending commercial email. In 1999, the United States passed the Anti Cyber Squatting Consumer Protection Act, which prohibits cybersquatting. The Information Technology Act of India lacks clear provisions for identifying and prosecuting cybersquatting, so these cases are resolved under the Trade Mark Act of 1999. As a result, the Anti-Squatting Rule must be implemented.

At the international level, there is a need to adopt clear and settled law on jurisdictional issues: The correct and systematic definitions of cyber-crime, as well as proper law on jurisdiction at both the national and international levels, are both in desperate need of clarification. In India, for example, there are only a few cases on cyber law and no major statutory schemes in place. When it comes to cyber-crime, policymakers and the courts are generally limited to referring to the scare current laws and cases. In situations where hackers store information on others' computers, on some webpage, or in their own e-mail address with a false name, the Information Technology Act of 2000 is unclear. Since hackers culture and modes of hacking are almost synonymous worldwide, whether in Russia, the United States, the United Kingdom, Canada, Australia, India, or anywhere else on the planet, there is a need to explain and settle this question. Cyber jurisdiction is a global problem in cyberspace. As a result, we must follow a uniform law on the question of jurisdiction; it must not be the case that a connection is sufficient to prosecute the case, since there might be a link with many countries. Companies whose systems or websites have been compromised by skilled hackers or cyber criminals should come forward and provide assistance to the Cyber Crime Investigative Cell or other organisations in order to deter further attacks. To fight and

monitor cyber hacking on a global scale, countries must work together at an international level.

The Convention on Cybercrime Must Be Signed and Updated: Any offence or contravention committed outside India by any individual, regardless of nationality, if the act or conduct constituting the offence or contravention involves a device, computer system, or computer network located in India, is subject to extraterritorial jurisdiction under the Information Technology Act, 2000. If a foreign national commits a crime punishable under the IT Act of 2000, the investigation, search, seizure, detention, prosecution, and extradition of cyber criminals will entail cooperation from concerned authorities in that foreign country. Since India is still not a signatory to the Cyber Crime Convention, which was opened for signatures on November 23, 2001 in Budapest, this becomes unlikely in the absence of a convention on cyber-crime for cooperation in cyber-crime matters. The Convention on Cyber Crime has designated cyber-crimes as extraditable offenses and can discuss extradition procedures. Owing to a lack of proper cyber laws on the issue of jurisdiction and a failure to sign the extradition treaty, the issue of jurisdiction in cyberspace remains unresolved. The cyber-crime convention must be signed. Even the United States and the United Kingdom have signed this Convention, which defines a number of crimes as extraditable, including: first, crimes against the confidentiality, integrity, and availability of computer data and systems, such as illegal access, illegal interception, data interference, system interference, and device misuse; second, computer-related crimes, such as computer-related fraud and forgery; and third, crimes against the confidentiality, integrity, and availability of computer data and systems, such as illegal access, illegal interception, data interference. However, the convention needs to be updated or ratified because it does not include all forms of cybercrime. There is also a need to update the list of extradition crimes under the Extradition Act of 1962 to include some other recent and increasing cyber-crimes that are common among cyber criminals and have an impact on a country's economic and social fabric. A treaty on international cyber law is also expected.

A Mutual Legal Assistance Treaty (MLAT) must be framed and updated: India has signed the Mutual Legal Assistance Treaty (MLAT) with a number of other countries for criminal cooperation, and it is also a signatory to the UN Convention against Transnational Organized Crime. Despite the fact that India has signed the MLATs and convention for criminal cooperation and legal assistance, cybercrime may be excluded from certain agreements that entail dual criminality and have no time limits for completing requests. Fast

action is required for proper investigation and prosecution of cyber-crimes, but it is believed that such a treaty would not provide an appropriate mechanism or structure for dealing with cyber-crime issues. It is necessary to make efforts to draft MLATs that specifically deal with international cooperation on cyber-crime issues, as well as to amend current MLATs with effective provisions, in order to achieve harmonization in substantive and procedural laws that regulate international cooperation on legal assistance in cyber-crime matters.

Recommendations Must Be Adopted and Enforced: The Standing Committee on Information Technology came up with this idea. On February 12, 2014, the Standing Committee on Information Technology released its fifty-second report on Cyber Crime, Cyber Protection, and the Right to Privacy, recommending that India's cyber security policy be urgently reformatted, as well as robust privacy legislation. The committee also recommended that the existing inadequacies of privacy protections in the Information Technology Act, as well as in Indian policies and practices regarding governmental projects and sensitive data and cyber matters, be highlighted. The committee also stressed the importance of enforcing section 43 A of the IT Act at the organizational level. The National Security Policy, 2013, has certain provisions, according to the committee, that may allow the creation of a legal structure to fill any holes that may exist. The committee also stressed the importance of periodic reviews of the IT Act because it lacks some protections for cyber security and cyber-crime, particularly in light of the recent controversy over Section 66A of the Act, and it also falls short in a number of areas. The importance of international cooperation in dealing with cyber security and cyber-crime must also be recognized, as the Centre for Internet and Society has pointed out, by upholding the concept of dual criminality.

It is also suggested that the United Nations system be instrumental in advancing global approaches to combating cybercrime and to procedures for international cooperation, with the aim of adopting the recommendation made by the United Nations General Assembly about the importance of putting special laws to deal with cybercrime, including for the United States of America and the United Kingdom, that the United Nations system should be instrumental in advancing global approaches to combating cybercrime and to procedures for international cooperation, with the purpose of It is also suggested that all states be encouraged to change their criminal laws as soon as possible to resolve the unique nature of cybercrime. It is also proposed that, in the case of conventional types of crime committed using emerging technology, certain laws that are no longer adequate be clarified or abolished

by introducing new provisions for new crimes or upgrading those that are no longer adequate. It is also proposed that states be encouraged to use the terms of the Council of Europe Convention on Cybercrime as a model for assessing the strength of new legislation.

The Need for Proper e-Courts Project and e-Learning Process Implementation:

The e-Courts project is based on the Supreme Court of India's e-National committee's Policy and Action Plan for Implementation of Information and Communication Technology in the Indian Judiciary, which was submitted in 2005 with the aim of transforming the Indian judiciary by enabling courts with information and communication technology and making justice delivery more affordable and cost effective. This Mission Mode project is one of the country's national e-governance initiatives, which is being implemented in the country's high courts and districts/subordinate courts. By March 2014, the government had authorized the computerization of 14,249 district and subordinate courts as part of this programme. This e-filing service is also available in the United Kingdom and the United States of America. Since October 2014, the United Kingdom has offered this e-filing service in the Chancery Division Court, and since June 2015, in the Admiralty and Commercial Court. Maryland, a US state, also offers e-courts, which will be available until June 2017 in the Southern Districts and Circuit Court of Maryland. The Hon'ble High Court of Karnataka announced in October 2014 that two e-courts will be created. This project is still not completely implemented across India, even in the area of cybercrime, and the general public is unaware of its existence. In this new era of enjoying the latest technologies all over the world, proper implementation of the e-Courts Project and e-Learning Process is needed at both the national and international levels, and efforts should be made to educate the general public.

The Indian Telegraph Act, 1885, must be amended: There are no legal guidelines in the Information Technology Act of 2000 for the crime of internet time theft. The Indian Telegraph Act, 1885, or Sections 378 and 379 of the Indian Telegraph Act, 1885, which describe the crime and provide penalties for theft, have not been amended. The Indian Telegraph Act of 1885 was passed with the purpose of allowing the government, as well as any company or individual licensed under section 4 of the Indian Telegraph Act of 1876 and specially empowered in this regard, to lay telegraph lines under or over private or public land. The Indian Penal Code, 1860, the Indian Evidence Act, 1872, the Bankers Book of Evidence Act, 1891, and the Reserve Bank of India Act, 1934 are all amended by the IT Act, 2000, but not the Indian Telegraph Act. As a result, it is necessary to amend the Indian Telegraph Act in order to make it more applicable in today's world.

Need for Clarity and Specificity in Penal Laws, rather than Relying on Vague Interpretations: Since the 1990s, cyberspace has grown in popularity and has had a rapid and negative effect on society. There is a need to pass penal laws with as much consistency and detail as possible in order to define ethical norms in cyberspace, rather than relying on ambiguous interpretations in current legislation, and criminals must be prosecuted for their clear actions. This must be accomplished on both a national and international scale.

Balance between law enforcement, adjudication, and correctional agencies is required: With technological advancements and globalization, a new medium has developed from which humanity is no longer able to differentiate between good and evil, national and foreign, just and unjust, but instead offers a forum for the events that occur in human society. Law is viewed as a regulator of human behavior that must enter cyberspace in order to address its numerous challenges. Despite this, further attempts must be made both online and offline by balancing law enforcement, adjudication, and correctional agencies. At both the national and international levels, there is a need to ensure coordination between three key components, namely law enforcement, adjudication, and correction, so that resources can be properly used and the justice process can run smoothly, and so that these can regularly function in a coordinated manner with the proper awareness of what the other segments are doing.

Need to Encourage Complaints against Cyber Crimes: Thousands of cases occur each year in different countries, but only a few are reported. Since many victims are afraid of being victimized in society, they do not file a lawsuit against cyber criminals. As a result, some cyber victims consider the incident as a nightmare, a bad fate, or a wish from God, and go on with their lives, forgetting about the incidents. However, cyber criminals are more encouraged to engage in certain types of cyber-criminal activities as a result of this. Since the private sector has been unable to disclose cyber-crimes for fear of negative publicity, which results in less judicial pronouncements, there is a great need to promote litigation at both the national and international levels. People's faith in law enforcement agencies' ability to fight cybercrime and in the Indian justice system's resilience in coping with new challenges in the cyber age is bolstered by conviction. Since the general public is unaware that a cyber-crime has been committed against them, they are unable to report it to the police. It is necessary to take proactive measures to encourage the general public and the private sector to come forward and assist the government in fighting these types of crimes.

Major Businesses Must Improve Their Cyber Resilience: Cybercrime and cyber security must be viewed as an ever-present threat by large corporations, necessitating ongoing investment and monitoring at the management and, most importantly, board levels. In the face of increasingly technically complex threats, major corporations must first ensure that sufficient cyber security is in place. Following that, companies must improve their cyber resilience, specifically their ability to detect, contain, and remediate breaches and other cyber incidents. Businesses are not only uninterested in implementing and maintaining the most up-to-date technological and high-demand practices, but they are also failing to evaluate how well they are equipped to tackle cyber-criminal attacks, as this testing would cover both their resistance to threats and their ability to minimize the damage or anxiety caused by cyber-attacks.

Partnership Approaches between Law Enforcement Agencies and Businesses are needed: Cybercrime is a dynamic and ever-increasing threat. Neither law enforcement nor companies would be able to minimize or regulate this threat on their own. To control cyber threats and recognize and disrupt cyber criminals, a partnership approach between law enforcement agencies and businesses is needed. Such collaboration will build on established intelligence sharing programs, such as sector-based information sharing forums and the government's Cyber Security Information Sharing Partnership, but would go even further in promoting and facilitating cyber-crime reporting, as proposed by the National Crime Agency (NCA).

The Need to Create a Common Agenda for Harmonizing the Atmosphere among Nations: The universal network is used by people all over the world on a national and international level, with the assurance that an international co-260 service exists. Every nation must create a common infrastructure for dealing with cyber-crimes that is compatible with the legal systems of other nations in order to preserve it. Many attempts are currently being made to create a shared agenda for harmonizing the environment between nations in order to tackle cybercrime through international treaties, conventions, or commissions, such as the UNCITRAL Model Law.

Government and public awareness are needed at both the national and international levels. It is also said that prevention is often preferable to cure. When using the internet, the general public should take some appropriate measures to protect themselves from such crimes. Since the public and government are both the pillars of a society, government and

public awareness are critical in combating the recent rise in cyber-crime on a national and international level. The government will make decisions based on what the public wants or needs. If they are the victims of a cyber-crime, they should report it to the police right away. The government will function better if the public is aware of their rights and responsibilities. The government should use technology-based programs, education, camps, and other useful ways to educate the general population about how to defend themselves from these types of crimes.

Cybercrime is also causing monetary and non-monetary damages to government and private sector agencies, departments, organisations, and other entities on a national and international level. There is a need to address this issue on both a national and international level, with private and public sector collaboration, as well as the development of investigative capabilities. Since there are few institutions in India that provide Cyber Crimes Investigation Training, there is a need to create more such institutions and to hold such camps on a regular basis. From time to time, technical training for police, cyber officials, investigative officers, lawyers, judges, and advocates is in high demand. The Indian police force lacks expertise in the highly technical area of computers and data networks. It is also proposed that, due to the highly competitive existence of information technology, law enforcement officials should cultivate a culture of continuous and learning education, since today's experience becomes redundant in a very short period of time.

To ensure Internet stability and multi-threat security systems, necessary measures must be taken. States should take the steps required to ensure Internet stability and protection in order to combat cybercrime and spam. There is also a need to safeguard and uphold the terms of the Universal Declaration of Human Rights and the Geneva Declaration of Principles relating to the right to freedom of speech and privacy. For the purpose of preventing and controlling cybercrime, national internet security standards must be high and of international quality. Government officials and departments, in particular, must use a Local Area Network (LAN) for internal correspondence, secrets, and sensitive information. There is also a critical need for public awareness, information technology education, and training among the general public, law enforcement, attorneys, judges, and government, as well as private organizations or institutions. For organizations to fight cybercrime on a national and international level, multi-threat protection systems and the implementation of foolproof computer procedures are needed.

Uniform Guidelines for Internet Service Providers and Cyber Cafés: There must be uniform guidelines for internet service providers and cyber cafés at both the national and international levels that expressly mention their liability and accountability, such as prohibiting them from using their clients' user numbers and maintaining the secrecy of their clients' information. These guidelines must be revised on a regular basis to reflect changes in circumstances.

Since email service providers fail to give two IDs to the same user, cyber criminals often provide false information when registering for an e-mail address with a website. This false and deceptive material on the internet aids the suspect in concealing his true identity and deceiving the authorities in locating the true perpetrator. Since the Information Technology Act makes no provision to prevent a person from registering for an e-mail address with a website by presenting false information, a person may create a false e-mail identity with a fictitious IP address and use it to commit a cybercrime. The I.T. (Amendment) Act, 2008 (10 of 2009) filled this gap in the Act by adding a new Section 66A into the main Act, which states that any fraudulent e-mail identity registration with a website is a crime punishable by up to two years in jail. It is unquestionably a step forward in the fight against cybercrime prevention and control.

Self-regulation can be proposed as a viable alternative for reducing the prevalence of cybercrime. It is the method of establishing a healthy code of conduct by both computer users and service providers following a policy of restraint. By implementing self-regulatory policies, Internet Service Providers (ISPs) will play a critical role in combating online crime. To begin, ISPs should establish a collective ethical code of conduct to be practiced by them when providing internet services and facilities to users. They may also set the terms in a written agreement that requires users to refrain from engaging in illegal activity. Furthermore, they will stipulate in the contract that any violation of these terms would result in the termination of internet services.

The government's regulatory framework for combating widespread cybercrime needs to be strengthened even further. Most significantly, current regulatory frameworks should enable law enforcement agencies to carry out their duties without fear of external pressure. Law enforcement authorities should be able to obtain any information they need from service providers in order to investigate internet crime without infringing on the parties' fundamental or privacy rights. The law relating to search, seizure, and detention as it applies to cyber-

offenses needs to be liberalized so that police or prosecuting agencies can detain cyber-offenders and bring criminal charges against them. The department of telecommunications should also review its policy against ISPs and place selective restrictions on them while expanding internet services by categorizing them based on their age, occupation, or status as an Internet Service Provider.

Indeed, technology is a strong weapon that has resulted in cybercrime. As a first step in preventing its misuse, places where computers are commonly used as a means of carrying out regular life tasks should be fitted with certain safety and protection devices to avoid unauthorized machine use. For example, a modern voice recognition system that activates based on voice pattern could be used effectively. Anomaly detection software, which detects suspicious patterns of computer use, aids users or organizations in responding to the intruder and frustrating him. Filter tech, likewise, has provided security against identified threats. Collar-ID technology in telecommunications as a security measure may also aid in the abolition of e-mail crimes. Filtering electronic mail from unwanted sites is also possible with similar technical devices.

Cyber forensic techniques must be established in order to provide significant technical assistance to the investigative agency in the identification, location, storage, and retrieval of digital information from a computer device in order to deliver it as cybercrime evidence in a court of law. Data forensics, cyber forensics, and software forensics are the three elements of the cyber forensics technique. Obviously, the three are intertwined to form a comprehensive cybercrime detection system. Computer forensics is the process of removing hidden or removed information from computer media confiscated at the scene of a crime in order to gather evidence. Cyber forensics, also known as network forensics, is concerned with digital evidence spread around a vast computer network. The main goal of cyber forensics is to find proof and establish the cyber criminal's motive and identity, as well as the effect of the crime on the victim(s). Software forensics primarily deals with the author of malicious code and provides significant clues to locate the perpetrator of cybercrime. The use of computer forensics as a method of analyzing legal evidence would undoubtedly aid cybercrime investigations and aid in locating the suspect and determining his guilt based on evidence obtained and presented against him in court. Biometric methods, like computer forensics, can be extremely useful in finding the true perpetrator of cybercrime.

Biometrics is the study of attributes derived from an individual's physical characteristics that are unique to that person. The codes obtained from electronic analysis of fingerprints, footprints, retinal scans, body odor, and other biometric data, for example, may provide useful clues to identify the individual suspected of cybercrime, but they must be backed up by other evidence.

One of the most important ways to combat cybercrime is to raise consciousness among computer users about the potential risks of using information technology for criminal purposes. It's all the more important because every network user is a potential target, and his lack of knowledge about information security and safeguards increases his vulnerability to cybercrime. As a result, raising awareness among computer owners and users through proper education can significantly aid in reducing the threats and damages caused by these crimes. Generally, internet users are unaware that when online, they may become victims of cybercrime or may unwittingly engage in an action that constitutes an offence, even though they did not plan to do so. This is especially true in the case of teenagers who, for the sake of amusement or fun, visit pornographic websites and occasionally become victims of such crimes. This risk can be avoided by informing internet users about the risks and repercussions of engaging in illegal activities on the internet, which they can unwittingly or ignorantly do. Some computer experts believe that a National Computer Crime Resource Centre, comprised of law enforcement personnel, forensic and legal experts, computer experts, members of the Central Bureau of Investigation, and members of the Reserve Bank of India, is urgently needed to collect, collate, and disseminate all data relating to computer crimes. In order to ensure secure computing, the center should also develop a model standard procedure.

It is widely acknowledged that intellectual property will be the real estate of the Third Millennium. The information technology revolution in the latter half of the twentieth century created new opportunities for IPR conflicts at both the national and international levels. To resolve these conflicts, a global Code of Digital Law must be created, with universal acceptance throughout the world. This is all the more important given the growing scope of IPR transactions with multi-national implications.

The perpetrators of cyber-crime are known to take advantage of flaws in the device that is being used or targeted. As a result, special protection measures can be implemented to discourage unauthorized computer device use. It is often claimed that domestic computer security legislation is primarily focused on ensuring public safety, security, and dignity rather

than providing sufficient protection to computer users, whether individuals or corporate entities. As a result, different countries' criminal laws, including cyber law, should be harmonized so that individuals, institutions, organizations, government and non-government entities, and society as a whole are adequately protected against the threat of cyber-crime.

Cyber terrorism is perhaps the most serious threat posed by computer systems and the internet. The advancement of information technology has allowed terrorists to obtain more advanced and disruptive technology and weapons to attack their targets, changing the conventional definition of terrorism. The harm caused by cyber terrorists is so severe and irreversible that it completely undermines national security and has a negative impact on the economy. Since cyber terrorism has now taken on international dimensions, it is necessary to combat the issue by improving e-security technologies and enacting strict penal policies at both the national and international levels. It has been suggested that India use the SAARC forum to help member countries reach agreement on the need for coordinated efforts to combat cybercrime, especially cyber terrorism, through regional cooperation. Efforts should also be made to obtain advanced cyber technology from developing countries through the adoption of a shared Cyber Legislation Code.

In September 1999, the Central Bureau of Investigation (CBI) announced the formation of a Cybercrime Investigation Cell, which began operations on March 31, 2000, in response to the demands of the time. The cell is led by a Superintendent of Police and covers the entire country. It has the authority to investigate the crimes mentioned in Chapter XI of the Information Technology Act of 2000, as well as other high-tech crimes. In India, six cybercrime investigation cells are currently operational, with headquarters in Delhi, Mumbai, Chennai, Bangalore, Hyderabad, and Kolkata. State governments are increasingly requesting the establishment of Cyber Crime Police Stations, similar to the CBI's Special Cyber Crime Investigation Cell. On August 30, 2001, the state of Karnataka became the first in the world to establish the country's first Cyber Crime Police Station, which has jurisdiction across the state. As a result, Cyber Police Cells were formed in major cities to deal with cybercrime. For the investigation of cyber-crimes, these cells are staffed by specially skilled and trained police officers who are assisted by computer specialists when required. However, most states lack dedicated cybercrime units, and cybercrime is managed by regular cops. As a result, it is proposed that each state establish at least one Special Cyber Crime Police Station, complete with electronic technology and computer-trained personnel, where cybercrime reports could be filed electronically and high-tech cybercrimes could be investigated easily and quickly.

With the approval of the concerned judge, police officers employed in these special cells should be able to scan publicly available data as well as data on private systems, computer devices, disks, and so on.

In terms of computer crime figures, they do not accurately represent the true occurrence of cybercrime. The explanation for this is that cybercrime is difficult to detect due to the operational speed and capability of computer software. Apart from that, many victims of computer crime refrain from reporting the crime for fear of being harassed and wasting time, energy, and resources in lengthy legal proceedings. Due to the fear of negative publicity, such as loss of reputation, humiliation, or unfavorable consequences, the trading community and businessmen are especially hesitant to disclose having been a victim of cybercrime. The lack of necessary technical resources on the part of law enforcement agencies to deal with cybercrime is also a contributing factor in victims' failure to report cybercrime incidents (s). The intangible existence of cybercrime, as well as the privacy of the victim, makes investigating cybercrime far more difficult. In conclusion, it can be concluded that cybercrime cases are seldom filed, and when they are, they are often dropped due to a lack of adequate evidence, or withdrawn or compromised by the parties-before they are eventually disposed of by the court. However, given the steadily rising incidence of cybercrime and the number of cases coming before the courts for adjudication, it would be worthwhile to begin publishing a Cyber-Crime Reporter or Cyber Law Journal for the benefit of members of the Bar Bench, police and enforcement agencies, and all those involved in the detection, investigation, and prosecution of cybercrime.

The Information Technology Act of 2000 requires transactions signed electronically to be recognized and enforced by law, but no system or device exists to determine when and exactly when a specific electronic document was prepared and signed electronically. Since no credible proof exists to determine the exact date and time that the contested electronic document was created and signed, there is ample room for doubt, which weakens the prosecution case in such cybercrimes. This issue can be solved by incorporating a digital device known as the Digital Time Stamping System (DTS) into electronic transactions. It consists of a device known as the Tamperproof Box, which uses a highly secure time-stamping server to produce digital time stamps (DTS). For several years, the scheme has been effectively operating in the United States.

Although the Indian information technology law recognizes cyber law's extraterritorial jurisdiction, it cannot be effectively enforced in cases where the perpetrator (usually a hacker) is located in a country with which India has no extradition treaty. This issue could be addressed by amending the law to allow cyber criminals from non-extradition countries to be brought to India for trial and prosecution in compliance with existing international law principles. Finally, it can be argued that in the twenty-first century's computer era, the internet has affected every aspect of human life, and no one can imagine life without computers. As a result, in the current situation, it is highly important that computer technology be retained for the advancement and prosperity of society rather than being misused by criminal conduits to commit crimes. In today's cyberspace, there are numerous websites that provide powerful tools for interacting, storing, and processing data.

As a result, web service providers should use care and patience when pasting details into their web pages. The ease with which data and information flows through the internet around the world can be used by criminals for the conduct of crimes, posing a significant concern for law enforcement agencies at both the national and international levels.

Today's society is becoming increasingly reliant on technology, and the number of crimes involving electronic devices is expected to rise. To keep crime at a minimum, the nation's law-making machinery should strive to be a mile ahead of the criminals. As a result, rulers and law makers should make constant efforts to ensure that regulating laws of technology include every aspect and problem of cyber-crime, and that they continue to evolve in a continuous and safe manner in order to keep constant vigil and check over the related crimes.