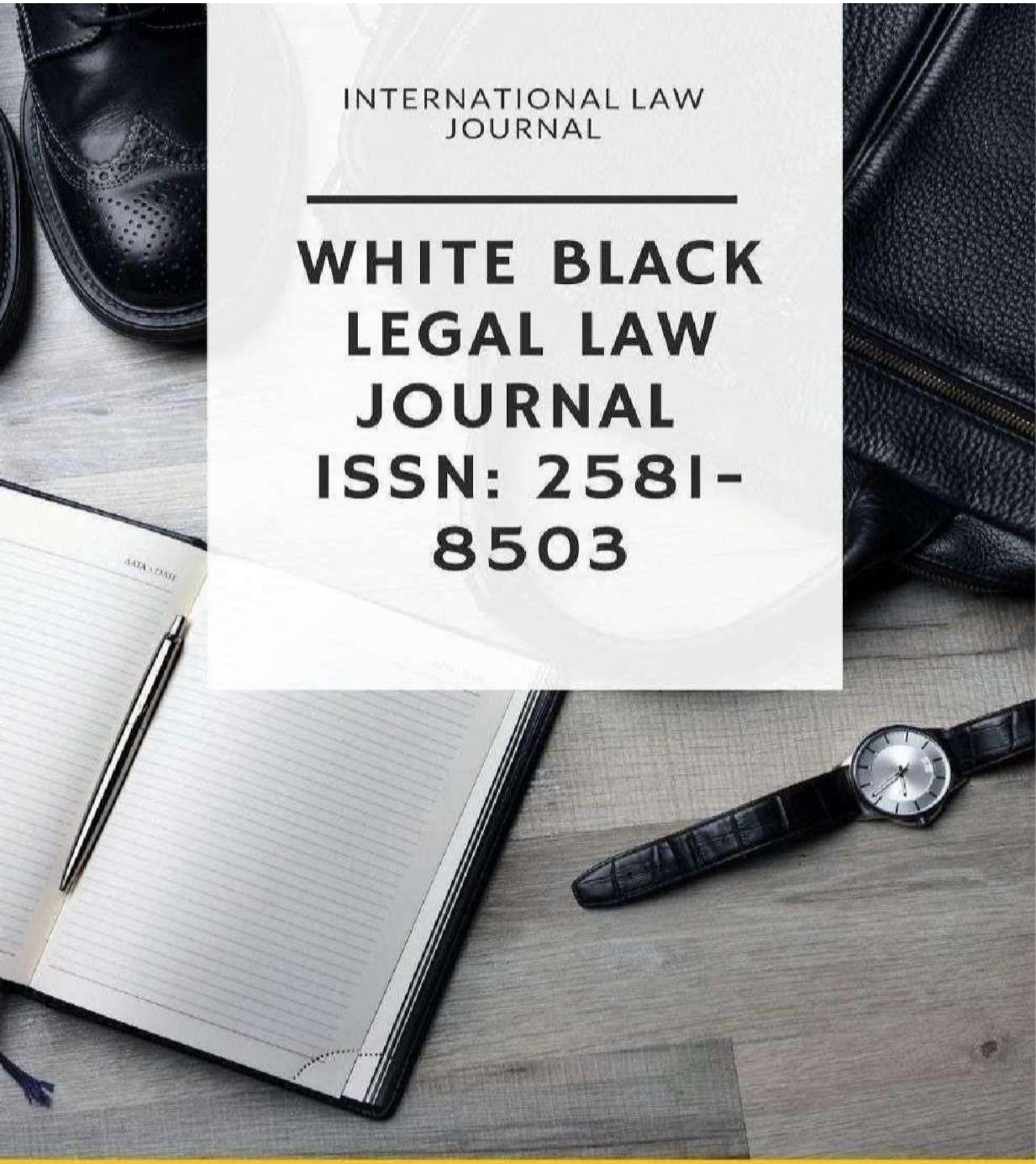

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

DISCLAIMER

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer

Dr. Raju Narayana Swamy popularly known as Kerala's Anti Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala . He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University . He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.

Senior Editor

Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,

Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Uttranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, Ph.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

A BRIEF STUDY OF CYBER LAW AND CYBER

CRIMES IN INDIA: INFORMATION TECHNOLOGY ACT, 2000

AUTHOREED BY - GAURAV GAUTAM
B.A.LL.B. (Hons.) II Year
thegauravgautam22@gmail.com
(8887263768)
ICFAI Law School, ICFAI University, Dehradun
2023 4360

"The modern thief can steal more with a computer than with a gun. Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb."

(National research council, USA "computers at risk".1991)

Abstract

With the evolution and development of technology over the past eras, there has been a tremendous increment in the usage of computers and mobile phones. The Internet has become so popular in providing a platform for communication and information supply.

The new boon that has been brought by this omnipotent information technology, bigot the scar in the form of cybercrime. The growth of these cybercrimes has propelled the need for stringent legal infrastructure like the **Information Technology Act, 2000** hereinafter IT Act which applies to the whole of India, including offences committed outside the territory deals with the cyber offences and electronic commerce in India. The act is inspired by the model legislation United Nation Model Law on Electronic Commerce adopted by the United Nation Commission on International Trade **(UNCITRAL)**.

The objective of the present work is to provide an overview of the provision of the IT Act, and the examination of the grey areas of the act.

Introduction

Since the inception of the internet era, services got cheaper people got exposed to the glamorized world of the internet which revolutionized the communication process, marketing process, etc. The web is a worldwide stage that is accessible to all anyone can easily become subject to this crime.

Large scale data get breaches from time to time, for reasons, including loss of sensitive data, system penetration by the intruders getting access to the sound and video capabilities of your computer which poses threat to one's privacy. The area of protection of privacy and personal data requires immediate attention.

Personal data is the Information of an identified natural person.[1]Misuse of such data violates the right guaranteed under the Indian constitution. Privacy as a right has evolved through the years. It was first recognized in the ***Kharak Singh v.The State of U.P. and ors***[2] and subsequently in 2017 given the status of Fundamental right in ***K.S. Puttaswamy and ors. v. Union of India and ors.***[3]

Cyberlaw and Cybercrime

Cyberlaw

Cyberlaw can be defined as the law governing the issues that are related to the utilization of technological devices like computers and the internet, or specifically the 'cyberspace'[4]. Oxford Dictionary defines cyberspace as

"The virtual environment in which communication occurs between computer networks"[5].

Cyberspace includes computers, software, storage data devices, the internet, and even electronic devices such as cell phones and ATMs, etc. Cyberlaw is the legal jurisdiction that regulates various aspects of the internet and computer security. Information Technology Act, 2000 regulates cyber laws in India.

Cybercrime

Cybercrime can be defined as the offences committed by the felon, where electronic

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council
[2] A.I.R. 1963 S.C. 1295.
[3] A.I.R. 2017 S.C. 4161.
[4] *Science Fiction Neuromancer* 1984, William Gibson
[5] http://www.oxforddictionaries.com/definition/english/cyberspace

communication devices, including the internet, are involved.[6]

The Indian law does not provide the definition of the term 'cybercrime'. It neither can be found in the **Information Technology Act, 2000** nor in the **I.T. Amendment Act, 2008.** The Indian Penal Code still does not use the term cybercrime even after the Amendment act of 2008.

India encountered a 300 percent increase in cybercrime cases between 2011 and 2014 and about 11,592 cases of cybercrime were registered in the year 2015.[7]

Categories of Cybercrime[8]

1. Against Person - Cyber Stalking, Impersonation, Loss Of Privacy, Transmission Of Obscene Material, Harassment With The Use Of Computer.
2. Against Property - Unauthorized Computer Trespassing, Computer Vandalism, Transmission Of Harmful Programmes, Siphoning Of Funds From Financial Institutions, Stealing Secret Information And Data, Copyright
3. Against Government - Hacking Of Government Website, Cyber Extortion, Cyber Terrorism, Computer Viruses
4. Other crimes - Logic Bomb, Spamming, Virusworms, Trojan Horse, E-Mail Bombing, E-Mail Abuse Etc.

Information Technology Act, 2000

The Information Technology Act, 2000 is the primary legislation that regulates the cyber offences of the cyber world in an effective manner. The then IT minister Mr. Pramod Mahajan finalized the bill and was passed by the former president of India K.R. Narayana on the 9th of May 2000. The Act gives legal recognition to E-commerce, Digital signature,[9]and Electonic Records.[10]

India is the 12th nation to enact this cyber law with the passage of the IT Act, 2000 which is based on the United Nation Model Law on Electronic Commerce adopted by the United Nation Commission on International Trade (UNCITRAL), 1996, to bring the uniformity in laws of

[6] https://cybercrime.org.za/definition
[7] https:// ncrb.gov.in/sites/default/files/crime_in_india_table_additional_table_chapter_
[8] Ms. Anjali Jolly, 2019, Cyber Laws in India, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) Volume 08, Issue 11 (November 2019),
[9] Section 5 of the IT Act, 2000.
[10] Section 4 of the IT Act, 2000.

different nations.[11] The Act originally had 94 sections divided into 13 chapters and 4 schedules. It applies to the whole of India[12]and the offences committed outside the territory of India.[13]

IT Act is made to lessen future legal issues and to harmonize the existing laws. Currently, two laws regulate the unethical activities occurring in cyberspace, which are the **Indian Penal Code,1860,** and **Information Technology Act, 2000.**

Objectives of the Act

a) To provide legal recognition to e-commerce.
b) To provide legal recognition to the digital signature.
c) To provide legal recognition to e-governance.
d) To provide a legal framework for electronic storage and data.
e) To provide punishments for cyber offences.[14]
f) To form the appealable agency the Cyber Appellate Tribunal.[15]
g) To amend the provision of certain statutes like IPC,1860, Banker's Book Evidence Act, 1891, the Indian Evidence Act, 1872, and the Reserve Bank of India Act, 1934.

To fill the loopholes in the cybercriminal justice system Information Technology Act 2000 brought certain relevant amendments in **sections 292, 294, 463, 464, 469, 503, 506**, of the IPC 1860[16], the Indian Evidence, 1872[17] making all the documents including digital records as lawful evidence in the court of law.[18] Banker's Book Evidence Act, 1891,[19] and RBI Act, 1934[20]provided the electronic fund transfer and enhanced the e-banking mechanism in India.

IT Act, 2000 covers offenses and penalties under chapters IX and XI. Also, it establishes the authorities for adjudication and investigation of cybercrime.[21] The offense under it is cognizable in nature which means if police found you as a suspect they can arrest you even without the warrant.

---

[11] http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model.html
[12] Section 1(2) of the IT Act, 2000.
[13] Section 75 of the IT Act, 2000.
[14] Chapter XI of the Information Technology Act, 2000 describes offences and punishment.
[15] Section 48 of the IT Act 2000
[16] First Schedule of the IT Act, 2000
[17] Second Schedule
[18] Section 3 of Indian Evidence Act, 1872
[19] Third Schedule
[20] Fourth Schedule
[21] Section 46 IT Act. Power to adjudicate

It primarily talks about the offenses such as hacking with a computer system,[22]which is a civil offense under **section 43** of the Act, tampering with the computer source code,[23] publishing vulgar or obscene data in the electronic form.[24]The offense of Phishing is punishable under **section 66C** of the IT Act with an imprisonment of 3 years and up to a 1 lakh fine. **section 66 and 72** of the Act provide for the crime of breach of privacy by way of cyber-stalking and online harassment.

Regulatory authorities under the Act

1. Department of Electronics and Information Technology

In India, the *Department of Electronics and Information technology* Under **Ministry of Communication and Information Technology** formulates policy and executes the law related to Information Technology Act. It has the power to appoint other regulating bodies like Adjudicating officers at the state level, Controller of Certifying Authorities, and Cyber Appellate Tribunal.

2. Adjudicating Officer

The Adjudicating Officer appointed by the central government at the state or UT level under **section 46** of the Act, is a qualified and experienced person to take the decisions in the matter of offenses, related to the Information Technology Act as well as in a position to determine the compensation of damages of IT Act, keeping the judicial mannerism in the view. [25]

3. Controller of Certifying Authorities (CCA)

The IT act by the virtue of **section 47** provides the controller of Certifying Authorities to regulated and license the working of Certifying Authorities, which issue the digital signature certificates to individuals. Safescrypt, IDBRT, TCS, MTNL, e-Mudhra, and even more are some of the Digital signature certifying authorities in India, which are subject to the IT Act, 2000.

4. Cyber Appellate Tribunal (CAT)

Section 49 of the IT Act, provides for the composition of the Cyber Appellate Tribunal under the aegis of Controller Certifying Authority (CCA). At first, the tribunal consisted of only one

[22] Section 66 IT Act. Hacking with computer system
[23] Section 65 IT Act. Tampering with computer source documents
[24] Section 67 IT Act.Publishing of information which is obscene in electronic form
[25] The Official Gazette of India, IT Act Notification no. 220 Available at https://www.meity.gov.in/content/it-act-notification-no-220

member as a presiding officer qualified to be the judge of the High Court. After the 2008 amendment changes were brought to section 49 which deals with the composition of the Tribunal and subsequently chairperson to be appointed and other members in the tribunal to be appointed by the central government.

For the purpose of discharging its function under the Act, The Cyber Appellate Authority (CAT) holds the same power, as vested with the Civil Court under **the Code of Civil Procedure, 1908**. It does not mandate the CAT to comply with the procedures of CPC, but it should follow the principles of natural justice. The proceedings of the Cyber Appellate Tribunal shall be deemed to be a judicial proceeding as per **sections 193**, and **228**, and for **section 196 of the Indian Penal Code**. For the purpose of **section 195 and Chapter 24 of the Code of Civil Procedure, 1973** Cyber Appellate Tribunal deemed to be the Civil Court

The parties discontent with decisions or the order of the Cyber Appellate Tribunal can file an appeal to the Hon'ble High Court within sixty days from the date of the decision CAT on any question of fact or law.[26]

5. Indian Computer Emergency Response Team (ICERT)

The Indian Computer Emergency Response Team (ICERT) mission is to improve the security of India's Communications and Information Infrastructure through proactive activity and viable coordinated effort. Its area of application is the Indian Cyber- community group. The reason for the ICERT is, to turn into the country's most confided agency of the Indian Community for reacting to PC security occurrences as and when they happen; the ICERT will likewise help individuals from the Indian Community in executing proactive measures to decrease the dangers of 100 computer security episodes.

ICERT has been designated under **section 70 of the Information Technology Act, 2000.** It gives specialized advice to system administrators and users to react to computer security episodes. It additionally performs the following function in the area of cybersecurity identifying the trend in the intruder's activity, forecast and alert the authorities of the new and upcoming cyber threats which could impose serious threats to cybersecurity, emergency measures to be taken to control the cybersecurity incidents. The team works with other organizations and institutions to resolve

[26] Section 62 of the IT Act, 2000 – Appeal to High Court

the cyber issues, disperses the data, guidelines white papers relating to IT practices.[27]

Information Technology (Amendment) Act, 2008

In order to keep up with the constant technological development, the IT Act was amended in 2008. Few changes were made in the IT Act, 2000 which brought improvement to certain provisions of the act. Following are the important changes adopted in the 2008 Amendment.

1. The term 'electronic signature'[28] has replaced the term 'digital signature' to make the act more amenable to technological development. Electronic signature means legal recognition of any electronic record by a subscriber by the means of technology.
2. The term 'communication device'[29] is defined under the new amendment. According to the definition communication device, it includes a digital communication device like a mobile phone or any other device that sends the information in the form of audio, video, or image.
3. The term 'cybercafé' was introduced through the amendment as the facility of access to the internet services by any person under a course of business to the public members.[30]
4. New sections added to the IT Act:

Section 66A authorized the power to arrest anyone who posts content that holds information of offensive nature or has menacing character. The penalty prescribed under the section was imprisonment up to three years with a fine.

Due to its vague and ill-defined definition, anything can be construed as offensive to anyone. Supreme Court in the case of ***Shreya Singhal v. Union of India***[31]declared this section unconstitutional as it violates the fundamental Right guaranteed under Article 19(1)(a) of the Indian Constitution.

Section 69A gives the power to the authorities to monitor, decrypt or intercept the data or information received, stored, or generated if it deems necessary to do so in the interest of the integrity, sovereignty, or security of the nation, to maintain the friendly relations with foreign nations. It empowers the central government to block internet websites if it deems necessary.

[27] ICERT, available at https://www.meity.gov.in/content/icert-0
[28] Section 2(ta) of the Information technology Act 2000
[29] Section 2(ha) of the Information technology Act 2000
[30] Section 2(na) of ITA 2008
[31] Shrey Singhal v. Union of India AIR 2015 SC 1523

Earlier in 2020 the government banned 118 Chinese apps under Section 69A of the IT Act to protect the interest of the citizen and the sovereignty and integrity of India.[32]

Case Laws

1. **State of Tamil Nadu v. Suhas Katti[33]**

This case is considered to be the first case under the IT Act, 2000 accused posted an obscene, defamatory message about the victim who is a divorced woman with a fake ID in the name of the victim only. Women filed a complaint against that annoying messages. The accused is found to be guilty of the offences under **section 67 of the IT Act, section 469,509 IPC.** Convict imposed with rigorous imprisonment along with the fine of Rs. 500 u/s 469 IPC, for the offence under 509 accused sentenced to simple imprisonment of 1 year and rigorous imprisonment of 2 years with a fine of Rs.4000 under section 67 of the IT Act.

2. **Syed Asifuddin case[34]**

TATA Indicom staff members were arrested for manipulation of the pre-programmed cell phones belonging to the Reliance Infocom and activated the TATA Indicom networks with all suspicious means. The court found all the accused held out to be liable under **section 65 of the IT Act**, which talks about tampering with computer source code.

3. **Avnish Bajaj v. State (NCT) of Delhi[35]**

Under the case there three accused one is the Avnish Bajaj CEO of a commercial portal, and the boy from Delhi school and IIT Kharagpur Ravi raj. Three sections were slapped against all the accused section **292, 294 of IPC 1860,** and section **67 of IT Act 2000.** In addition, the schoolboy was charged under section 201 of IPC for destroying the evidence. Later Avnish Bajaj was acquitted for his due diligence and the Delhi schoolboy was granted bail by the Juvenile Justice Board and was kept under home surveillance for 2 days.

Conclusion

[32] http://www.pib.gov.in
[33] CC No.4680 of 2004
[34] Syed Asifuddin and ors. v.State of Andhra Pradesh and Anr.2005 CriLJ 4314
[35] (2008) 150 DLT 769

The adoption of the Information Technology law has contributed to the growth of trade, e-commerce, and the law-enforcing authorities that deal with cyber offences effectively and make our nation more technologically vibrant. However, the IT act has some grey areas, which require new legislation that can cover all the lacuna in the existing law.

- The Act, 2000 is likely to cause dispute in the matter of territorial jurisdiction since cyber offences are internet-based crimes.

- The IT Act does not talk about any issues of intellectual property rights in the online environment. Issues concerning online patents, trademarks, and copyright are left untouched and need urgent cognizance.

- Where cybercrimes are taking new forms and manifestation, our IT act does not even have a set definition of cybercrime and the offences defined under the act are by no means exhaustive.

- The existing laws are limited to the theoretical punishments as it is difficult to prosecute the anonymous criminal, the crime committed in the dynamic virtual space, and the destruction of the evidence is easy. A specialized procedure to deal with such crimes is to be ensured.

References

1. Regulation (EU) 2016/679 of the European Parliament and of the Council
2. A.I.R. 1963 S.C. 1295.
3. A.I.R. 2017 S.C. 4161.
4. *Science Fiction Neuromancer* 1984, William Gibson
5. http://www.oxforddictionaries.com/definition/english/cyberspace
6. https://cybercrime.org.za/definition
7. https:// ncrb.gov.in/sites/default/files/crime_in_india_table_additional_table_chapter_
8. Ms. Anjali Jolly, 2019, *Cyber Laws in India*, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) Volume 08, Issue 11 (November 2019),
9. Section 5 of the IT Act, 2000.
10. Section 4 of the IT Act, 2000.

11. http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model.html
12. Section 1(2) of the IT Act, 2000.
13. Section 75 of the IT Act, 2000.
14. Chapter XI of the Information Technology Act, 2000 describes offences and punishment.
15. Section 48 of the IT Act 2000
16. First Schedule of the IT Act, 2000
17. Second Schedule
18. Section 3 of Indian Evidence Act, 1872
19. Third Schedule
20. Fourth Schedule
21. Section 46 IT Act. Power to adjudicate
22. Section 66 IT Act. Hacking with computer system
23. Section 65 IT Act. Tampering with computer source documents
24. Section 67 IT Act.Publishing of information which is obscene in electronic form.
25. The Official Gazette of India, IT Act Notification no. 220 Available at https://www.meity.gov.in/content/it-act-notification-no-220
26. Section 62 of the IT Act, 2000 – Appeal to High Court
27. ICERT, available at https://www.meity.gov.in/content/icert-0
28. Section 2(ta) of the Information technology Act 2000
29. Section 2(ha) of the Information technology Act 2000
30. Section 2(na) of ITA 2008
31. Shrey Singhal v. Union of India AIR 2015 SC 1523
32. http://www.pib.gov.in
33. CC No.4680 of 2004
34. Syed Asifuddin and ors. v.State of Andhra Pradesh and Anr.2005 CriLJ 4314
35. (2008) 150 DLT 769