

ISSN: 2582-6433



INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed 6th Edition

VOLUME 2 ISSUE 7

www.ijlra.com

DISCLAIMER

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Managing Editor of IJLRA. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of IJLRA.

Though every effort has been made to ensure that the information in Volume 2 Issue 7 is accurate and appropriately cited/referenced, neither the Editorial Board nor IJLRA shall be held liable or responsible in any manner whatsoever for any consequences for any action taken by anyone on the basis of information in the Journal.

Copyright © International Journal for Legal Research & Analysis

IJLRA

EDITORIAL TEAM

EDITORS

Megha Middha



Megha Middha, Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar

Megha Middha, is working as an Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar (Rajasthan). She has an experience in the teaching of almost 3 years. She has completed her graduation in BBA LL.B (H) from Amity University, Rajasthan (Gold Medalist) and did her post-graduation (LL.M in Business Laws) from NLSIU, Bengaluru. Currently, she is enrolled in a Ph.D. course in the Department of Law at Mohanlal Sukhadia University, Udaipur (Rajasthan). She wishes to excel in academics and research and contribute as much as she can to society. Through her interactions with the students, she tries to inculcate a sense of deep thinking power in her students and enlighten and guide them to the fact how they can

bring a change to the society

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board



Dr. Namita Jain



14th, 2019

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC - NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India. India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020). Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi. Formerly Assistant professor of Law, Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration. 10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.



Avinash Kumar



methodology and teaching and learning.

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship. He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi. Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi. He has qualified UGC - NET examination and has been awarded ICSSR - Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS
ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

CYBER CRIME: LAWS & **PUNISHMENTS**

*Authored By: Ronith Raj C.S
& Ahmned Hannan Anwar
Alliance School Of Law,
Alliance University Bangalore*

ABSTRACT:

This paper focuses about cybercrime, the laws made to stop cyber crime and punishments involved in the same. Cyber crime is a leading headline in the 21st century or famously known as the technological era, the crime rate with the usage of Artificial Intelligence (AI) and internet has skyrocketed, the fear instilled in people made us think twice before using any kind of technological devices or opening any kind of websites. Internet, as useful and simple as it seems, it is at the same time the most dangerous and a platform which makes the people vulnerable to the loss of their details, privacy and even wealth.

The paper will also be focusing on some of the leading cases related to cybercrime such as:

- a) Shreya Singhal v. UOI
- b) Avnish Baja v. State (NCR) of Delhi

And further we will look into the Information Act 2000, the enactment, the punishments, the advantages. Many section involved under Indian Penal Code (IPC) and the prominent cases under the sections.

CHAPTER 1: INTRODUCTION

Cyber-crime is a leading problem in every nook and corner of the world as we live in a digital era. Ever since the invention of the World Wide Web (WWW) people found it very helpful and advantageous in many ways for e.g.; if you wanted to know about a specific thing all you had to do was type it in and within a span of seconds every single interpretation of the said topic will be available in front of you or if you wanted to cure boredom you can play games or watch movies and entertain yourselves.

Internet has made possible those things which were unimaginable a few years ago. The internet is becoming a fast way of living for billions of people and everyone is basically dependent on the internet for each and every job as there is a huge reliance on these machines for every aspect of work. But with the advantages of use of internet also comes the disadvantages of it. With the daily use of internet in every aspect of life there is a greatest disadvantage of internet i.e., cyber-crime. Cyber-crime means crime done with the help of computer or internet where computer is used as a tool or as the target and includes everything from hacking a system to denial-of-service attacks. Cyber-crime has been reported around the globe and is now among the most important revenue sectors for crimes organised globally

The World Wide Web was praised by man-kind for its technological prowess and its high speed problem solving mechanics and so on, but this praising had to come to a stop a few years later as the internet evolved and people came up with apps and websites to make it more interesting for the people and to make money out of it. This idea was applauded as it made the lives of everyone easier as it helped people connect with each other no matter how far they live from each other (social media) and also lend a hand in acquiring knowledge and information just in seconds. But as people say, "Life is not always unicorns and rainbows" and this was proven right by the people itself, as all the websites and apps that we log into and use takes in our details such as; email address, Ip address, contact info and so on. This took a very bad turn after rumours started spreading that "all the data are being sold to the highest bidder" and it turned out to be true and instilled fear in people.

This became more serious when people started hacking into social media accounts, bank accounts, social security numbers and many more which further resulted in theft, identity theft, false accusation, impersonation and cyber bullying. The number of crimes committed through

the usage of technology increased it became a huge headline without much time, and Cyber Crime was introduced.

Cyber crime is noted under The Information Technology Act, 2000 also known as the ITA 2000 or IT Act. This is the first cyber law in India that provides a legal infrastructure of e-commerce in India. This act was enacted on 9th of June 2000 but came into effect on the 17th of October 2000. Cyber-crimes were further mentioned in Section 499 of IPC – sending defamatory messages by email, Section 463 of IPC – Forgery of records, Section 40 of IPC – cyber frauds and Section 463 of IPC – email spoofing. The IT act has been enacted which ensure complete privacy of the citizens details and this was made clear when Shiv Shankar Singh stated “Each person must be able to exercise a substantial degree of control over their own data and its use”. This act also defines cyber crimes and the penalties for the same. Cybercrime can also be seen connected to normal IPC violations such as:

Defamation: You can defame a person through messages, images, or videos.

Threat: many cases were filed regarding cyber threats and or cyber bullying.

1.1. NOTABLE CASES UNDER CERTAIN SECTIONS

SECTION 66A:

“This section criminalises the sending of offensive messages through a computer or other communication devices”.

CASES:

- In September 2012, a freelance cartoonist Aseem Trivedi was arrested under the Section 66A of the IT Act, Section 2 of Prevention of insults to national honour act, 1971 and its sedition under the Section 124 of the Indian Penal Code. "His cartoons depicting widespread corruption in India were considered offensive." (“Information Technology Act, 2000 - Wikipedia”)
- On 30 October 2012, Puducherry businessman Ravi Srinivasan was arrested under Section 66A. "He had sent tweet accusing Karti Chidambaram, son of then Finance Minister P. Chidambaram, of corruption." (“Information Technology Act, 2000 - Wikipedia”) Karti Chidambaram had complained to the police.

- SHREYA SINGHAL v. UOI:

Two women were arrested under section 66a of the IT act after they posted allegedly offensive and objectionable comments on Facebook concerning the complete shutdown of Mumbai after the demise of a political leader. The women in response to the arrest filed a petition challenging the constitutionality of section 66A on the ground that it is violative of the freedom of speech and expression.

The court based its decision on 3 concepts: discussion, advocacy, and incitement. It was found that section 66A was capable of restricting all forms of communication and it contained no distinction between mere advocacy or discussion on a particular cause which is offensive to some and incitement by such words leading to a causal connection to public disorder.

SECTION 69A:

“Power to issue directions for blocking of public access of any information through any computer resource.”

CASES:

- On 29 June 2020, the Indian Government banned 59 Chinese mobile apps, most notably Tik Tok, supported by Section 69A and citing national security interests.
- On 24 November 2020, another 43 Chinese mobile apps were banned supported by the same reasoning, most notably AliExpress. 54 more apps including popular video game Garena Free Fire were banned on 14 February 2022 under the same section.

SECTION 67:

“Punishment for publishing or transmitting obscene material in electronic form.” (“Punishment for publishing or transmitting obscene material in ...”)

CASES:

AVNISH BAJAJ v. STATE (NCR) OF DELHI:

Avnish Bajaj, the CEO of bazee.com was arrested under Section 67 of IT act for broadcasting of cyber pornography. Someone else had sold copies of a CD containing pornographic material through the bazee.com website.

LITERATURE REVIEW

- Catherine D. Marcum, Cyber Crime, Criminal Justice Series, Second Edition

https://www.google.co.in/books/edition/Cyber_Crime/DReGDwAAQBAJ?hl=en&gbpv=1

This provides us with a clear and thorough examination of the prominence of cybercrime in our society, as well as justice system experience with cybercrimes. Research from scholars in the academic field, as well as government studies, statutes, and other material are gathered and summarized the key concepts, statistics and legislative histories are discussed in every chapter. The book is meant to educate a wide audience about the existing cyber crimes and the possibility to fall into the trap and be a victim of it. This text should be helpful to students, academic, and practitioners alike.

- Prof. Dr. Anita Singh, Prof. Dr. Pradeep Kulshrestha, Prof. Dr. Ritu Gautam, Cyber Crime, Regulation and Security: Contemporary Issues and Challenges

https://www.google.co.in/books/edition/Cyber_Crime_Regulation_and_Security_Cont/1TGKEAAAQBAJ?hl=en&gbpv=0

in the era of a fast- changing technically driven society, to make life easy and simple people use various devices. The internet is one of the easiest and most economical modes of connecting people and businesses across the world. Usually, it is believed that a computer has been used as a medium or instrument for the commission of cybercrimes like trespass, larceny, or conspiracy on the other hand much credence is given to the unique nature of emerging technologies and unique set of challenges, unknown to the existing cyber jurisprudence, such as nature and scope of cybercrimes, intention, and difficulties in the locating the offender, jurisdiction and its enforcement

- Talat Fatima, Cyber Law in India

https://www.google.co.in/books/edition/Cyber_Law_in_India/9IyWDwAAQBAJ?hl=en&gbpv=0

Derived from the renowned multi-volume International Encyclopaedia of Law, this practical guide to cyber-law, the law affecting information and communication technology (ICT), in India covers every aspect of the subject, including intellectual property rights in the ICT sector,

relevant competition rules, drafting and negotiating ICT-related contracts, electronic transaction, privacy issues, and computer crime. Lawyers who handle transnational matters will appreciate the detailed explanation of specific characteristic of practice and procedure.

SCOPE AND OBJECTIVE

- 1) Understanding Cyber-Crime.
- 2) Understand why spreading awareness regarding cybercrime is necessary.
- 3) Elaborate the advantages of Cybercrime Law in India.
- 4) Know about the punishments and laws implemented in India regarding cybercrime.

RESEARCH PROBLEM

Unauthorised access to other networks, harassment via e-mail, cracking, hacking, page jacking, carding, cyber-stalking and many more cybercrime. Some of the most known cybercrimes include identity theft, ransomware, cyber extortion, phishing, data breach, online shopping scams, etc. the ill effects of cybercrimes often lead to extreme financial ruin and reputation loss to both businesses and individuals. Cyber laws address and deals with many issues, such as racism, online insults, gender targets to protect a person's reputation. Harassment is a major issue in cyber space¹, which is a violation of both criminal laws and civil. In cyber law, there are some hard laws defined to prohibit these kinds of despicable crimes. Apart from this, the main problem that we come across is the lack of awareness within the society about the threats and vulnerability when using technological appliances and AI subjects, as there is no national regulatory policy in place for cybersecurity there is a lack of awareness at both company level as well as individual level. Domestic netizens can protect and be protected from the cyber attacks only if there is a guided and supervised legal framework.

Major challenge to cyber ethics is confidentiality which is a key ethical issue in cybersecurity. Security professionals will, by the nature of their profession, see and handle personal, private or proprietary information that should be kept strictly confidential.

¹ Cyber space is a space that epitomizes technological development, at the same time highlighting the uncertainty regarding legal issues that arise from it.

RESEARCH QUESTIONS

- 1) Ethical problems with having cyber-crime law in India?
- 2) How relevant is cyber-crime in India?

HYPOTHESIS OF THE STUDY

After going through several articles and books in regard to Cybercrime it is can be understood that Cyber laws in India needs to be more strict and the public or citizens should have proper awareness about the threats that can possibly attack them.

RESEARCH METHODOLOGY

Since the study requires collecting data from multiple sources, it will adhere to the doctrinal approach. Primarily secondary sources are used. All available books, journals, and papers were read. Published books and papers are the gold standard for research. The following strategies will be used to achieve the study's goals and gather the required data.

- Study of the existing books.
- Books, journals, and articles may serve as both secondary sources.
- Internet surfing

IJLRA

CHAPTER 2: ETHICAL PROBLEMS WITH CYBER-CRIME LAW IN INDIA

Cyber security practices aim to secure computer systems and networks and keep data safe. Those, data, system, and networks indeed hold some economic or other value in themselves, but what security practices essentially protect is the integrity, functionality, and reliability of organizations that rely upon such data and systems. The following are the three important ethical issues in cyber security: (“A Holistic Approach to Ethical Issues in Cyber Security”)

HARM TO PRIVACY:

Privacy harm is conceptualized as the negative consequence of a privacy violation. The exposure of sensitive personal information results in costly spam, phishing, or other undesirable communications. The said, it is important to understand that privacy harms do not jeopardize those whose sensitive information is directly exposed to cyber threats. "Even those who try to live disconnected from the digital cannot prevent sensitive data about them from being generated and shared by their friends or family." (“A Holistic Approach to Ethical Issues in Cyber Security”)

TRANSPARENCY AND DISCLOSURE:

Cyber security is a form of risk management, and because those risks substantially affect other parties, there is a default ethical duty to disclose those risks when identified, therefore affected parties can make informed decisions. For instance, if a company finds out a critical vulnerability in its software, it must notify its customers or clients of that discovery in a timely manner.

LACK OF SEPARATION:

Unlike countries or states, in cyberspace there are no boundaries, thus making the armed assets of ONGC², banking functions, etc, vulnerable to cyber attacks from anywhere. This could result in security breaches at a national level, causing loss of money, property, or lives.

Although cyber ethics remains an under-researched field, we tried to shed light on ethical issues in cyber security. Ethics have always been important in the past, however, the awareness of ethics is becoming more critical now. Cyber security professionals and organizations should adopt procedures for rigorously evaluating the compliance of their members with the applicable ethical cyber security obligations.

² Oil and natural gas co-corporation

CHAPTER 3: HOW RELEVANT IS CYBER CRIME IN INDIA?

"Cyberlaw responds to the unique challenges of the Internet and other digital technologies." ("Brief Guide To Understand The Importance of Cyber Laws in India") These technologies have created new opportunities for criminals, cyberbullies, and others who would exploit the technology for their purposes. At the same time, they have also created new ways for people to share information and ideas and connect. Cyber laws exist to protect people from online frauds. They exist for preventing online crimes that include credit card theft and identity theft. A person who commits such thefts stands to face federal and state criminal charges.

Cyber law is a term used to describe the legal aspects of using technology, particularly the internet. It covers various topics, from copyright and trademark law to data protection and privacy. These laws govern how information is collected, used, and stored. They are designed to protect people's privacy and prevent the misuse of personal information. Other important cyber laws include those that deal with copyright and trademark law.

These laws protect the intellectual property rights of creators and owners of copyrighted material. They are designed to prevent others from using or copying material without permission. Still, other cyber laws govern the use of electronic commerce or e-commerce. These laws govern the transactions that take place online, such as the purchase of goods and services. They protect consumers and businesses from fraud and other illegal activities.

3.1. Key takeaway for cyber law in India

1. Cyber law is a new and constantly evolving area of law.
2. Cyber law covers a wide range of legal issues including, but not limited to, cybercrime, data protection, privacy, and e-commerce.
3. Cyber law is important in India because of the growing internet users and the increasing reliance on technology.
4. Cyber law is important for businesses operating in India because it helps them to comply with the law and avoid legal liability.
5. Cyber law is also important for individuals because it helps them to understand their rights and responsibilities online.

CHAPTER 4: CONCLUSION

There is no one “cyber law” but a collection of laws and regulations that govern the use of technology. These laws are constantly evolving as modern technologies are developed, and new ways of using them are found. Some of the most important cyber laws deal with data protection and privacy. In general, the future of cyber law in India is likely to be shaped by several factors, including the increasing use of technology, the globalization of business, and the growing threat of cybercrime. As technology advances and more people rely on the internet to store sensitive information such as banking or credit card information, criminals increasingly attempt to steal that information. Cybercrime is becoming more of a threat to people across the world. Raising awareness about how information is being protected and the tactics criminals use to steal that information continues to grow in importance. But cybercrime does not yet seem to be on the average person's radar. (“Cybercrime - Wikipedia”) There are 1.5 million cyber-attacks annually, which means that there are over 4,000 attacks a day, 170 attacks every hour, or nearly three attacks every minute, with studies showing that only 16% of victims had asked the people who were carrying out the attacks to stop. In India as well as across the globe, with the increasing reliance of humans on technology, cyber laws need constant up-gradation and refinement to keep pace. There has also been a significant increase in the number of remote workers as a consequence of the pandemic, which has increased the need for application security. There is a need for legislators to take extra precautions to keep ahead of the imposters so that they can act against them as soon as they arise. It can be prevented if lawmakers, internet providers, banks, shopping websites and other intercessors work together.

PENALTIES:

- Tampering with the documents stored in a computer system³: Imprisonment of 3 years or a fine of Rs.2 lakhs or both.
- Receiving a stolen computer source or device dishonestly⁴: Imprisonment for 3 years or a fine of Rs.1 lakh or both.
- Identity theft⁵: Imprisonment of 3 years or a fine of Rs. One lakh or both
- Cheating by personation⁶: Either imprisonment for 3 years or a fine of Rs. One lakh or both.
- Violation of privacy⁷: Either imprisonment up to 3 years or a fine of Rs. Two lakhs or both
- Cyber terrorism⁸: Life imprisonment

³ SECTION 65

⁴ SECTION 66 B

⁵ SECTION 66 C

⁶ SECTION 66 D

⁷ SECTION 66 E

⁸ SECTION 66 F

CHAPTER 5: REFERENCES

- <https://blog.ipleaders.in/information-technology-act-2000/#:~:text=Imprisonment%20of%203%20years%20or,act%20mentioned%20in%20Section%2043.&text=Imprisonment%20of%203%20years%20or%20a%20fine%20that%20extends%20to%20Rs.>
- <https://enhelion.com/blogs/2021/03/01/landmark-cyber-law-cases-in-india/>
- <https://khatabook.com/blog/article-1019-importance-of-cyber-law-in-india/#:~:text=Importance%20of%20Cyber%20Law%20in%20India,-Cyber%20Law%20is&text=The%20primary%20objective%20of%20Cyber,legal%20recognition%20for%20electronic%20transactions.>
- <https://www.njlrii.com/2022/06/ethics-and-cyber-crimes-in-india.html>
- https://en.wikipedia.org/wiki/Information_Technology_Act,_2000#:~:text=The%20Information%20Technology%20Act%2C%202000,with%20cybercrime%20and%20electronic%20commerce.
- <https://enhelion.com/blogs/2021/03/01/landmark-cyber-law-cases-in-india/>
- https://en.wikipedia.org/wiki/Shreya_Singhal_v._Union_of_India#:~:text=Section%20066A%20of%20the%20Information%20Technology%20Act%2C%202000%20made%20it,computer%20resource%20or%20communication%20device.

IJLRA