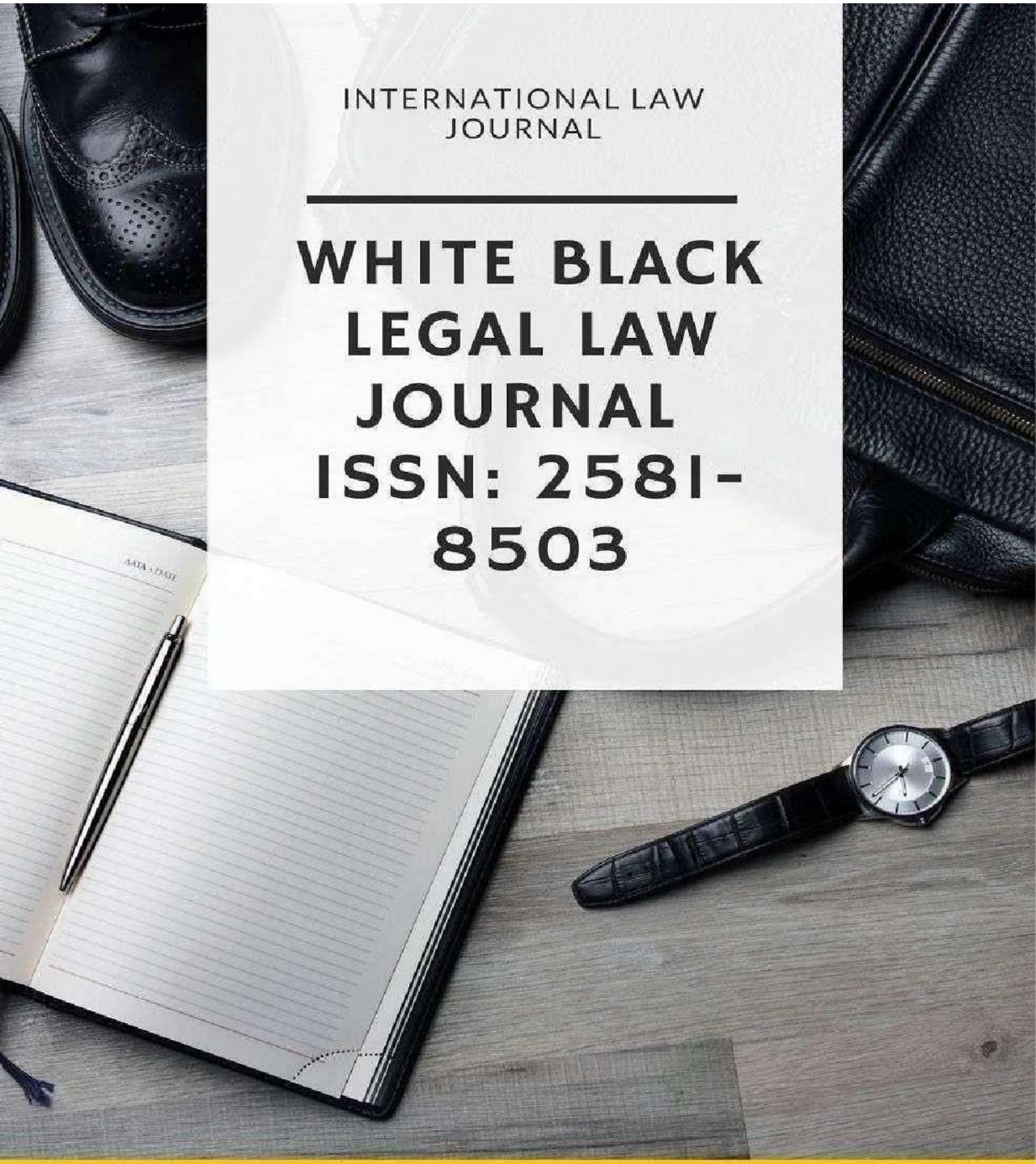


INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

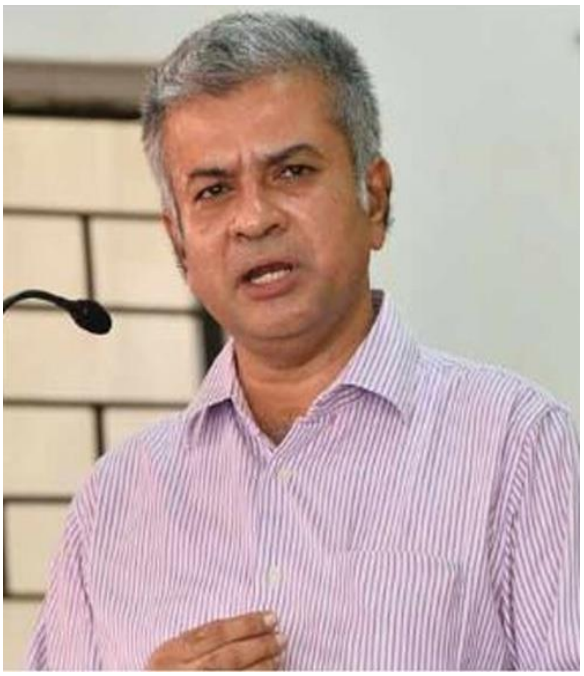
Peer - Reviewed & Refereed Journal

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

CYBER -TERRORISM

AUTHORED BY - PRIYANKA SETHI

Abstract

As India is rapidly becoming a global leader in IT, it is also becoming a significant target for cybercrime, with more and more innocent people falling prey to these attacks every day. When this happens, it's crucial to safeguard citizen rights against crooks who prey on the uninformed. Cyberspace has accelerated the development of all technologies to such an extent that it has widened the knowledge gap between generations. The wealth gap in India is wide, and the nation also has high poverty and literacy rates. As a result, the divide between the generations widens even more for these reasons. Because of how difficult it is to maintain tabs on activity in the virtual world, it is incumbent upon legislators and law enforcers alike to develop an effective legislative system for dealing with cybercrimes. So, the purpose of this study is to undertake an analysis of the legal system in order to get an appreciation for how well it regulates cybercrimes in India.

1. INTRODUCTION

Since the advent of the internet, the number of people using it has been steadily growing all over the world. Even in India, the number of people who use the internet is growing, and surprisingly, India has surpassed the number of people who use the internet in the United States. The number of people who use the internet in the United States accounts for only 4.4% of the population of global internet users, while the number of people who use the internet in India accounts for 17.2% of all total global users Because the vast majority of people who use the internet in India are under the age of 30, this demonstrates that the Indian workforce is fundamentally dependent on IT-based technologies.[1] This reliance is a primary factor in why India's IT and BPO sectors are now among the most prominent in the world. But, it is also important to recognize that the internet has given rise to a globalized, borderless, and mostly unregulated virtual world. Indeed, this is an issue that needs consideration. Several different kinds of activity, some of which may not be easily traceable back to their origin, are made possible by the internet.[2] This makes it difficult to enforce laws and keep the online world safe in ways that make sense in the real world. So, this

[1] Jyoti Rattan, "Cyber Laws & Information Technology" (Bharat Law House Pvt. Ltd., New Delhi, 4th edn., 2014).
[2] . Kamal Ahmad: The Law of Cyber-Space (U. N. Institute of Training & Research) 2006

paper will attempt to evaluate the Indian legal framework on the subject of cybercrime regulation in the online cyber world. The current era of rapid digitization makes this even more crucial.[3]

2. CYBER CRIMES AND CYBER OFFENCE

The word "cybercrime" is often used to describe any illegal behaviour that is committed via a sequence of electronic operations with the goal of compromising the security of computer systems or the data stored inside them. However, in a broader sense, the word "cybercrime" may be used to refer to any unlawful behaviour or actions using a computer system or network. The holding of information, as well as its provision, diffusion, or exchange through such computer systems or networks, falls within this definition. The Budapest Convention is the first instrument of international law whose principal purpose was to create a uniform set of laws at the global level for combating various cyber offences.[4] The convention was created for this same reason. It was so groundbreaking that it was the first legal mechanism to link cybercrime to violations of human rights.

According to the definitions that are supplied by this Convention, the most prevalent sorts of cyber crimes include data interference, unauthorised access, misuse of equipment, illegal interception, computer-based fraud or forgery, offences associated with copyright, neighbouring rights, and child pornography. These are the types of crimes that are most likely to be committed. With the adoption of an Additional Protocol to this Convention, it became illegal to distribute any literature that promoted racism or xenophobia. Similarly, this Agreement forbids the publication of such data. The scope of this Agreement has been expanded to include acts of terrorism perpetrated online. Given these realities, one may argue that cybercrime encompasses not only those crimes perpetrated over the Internet but also those carried out using mobile phones, networks, and other electronic devices[5]. Even crimes that aren't performed through computers or networks per se may fall under the umbrella of "cyber offences" if they are committed with the intent to disrupt or damage computer systems. Conversely, no piece of Indian law, not even the Information Technology Acts of 2000 and 2008, defines cybercrime or other online offences with any degree of specificity. Hence, it is crucial to investigate the provisions of numerous laws dealing with cyber offences, as well as the many types of cyber offences that have taken place or been committed in India.

---

[3] Nandan Kamath, Law relating to Computers, Internet and E-Commerce: A Guide to Cyber Laws and the Information Technology Act, 2000 (Universal Law Publishing Co., New Delhi, 2nd edn., 2009).
[4] Pavan Duggal, “Cyber Law An exhaustive section wise Commentary on the Information Technology Act along with Rules, Regulations, Policies, Notifications etc”, Universal Law Publishing - An imprint of LexisNexis (2014)
[5] R. Nagpal : What is Cyber Crime ; (2003)

3. A LEGAL FRAMEWORK FOR CYBER CRIMES AND OTHER CYBER OFFENSES IN INDIA

The Information Technology Act of 2000, which was recently revised in 2008, is the primary piece of Indian law that addresses offences using computers. This act came into effect in 2000. Nonetheless, statutes such as the Indian Criminal Code 1860 and the Indian Evidence Act 1972, amongst others, do have some broad provisions connected to cyber offences. Certain provisions in these laws have even been added to address issues raised by advances in information technology. According to the IT Act's stated goals, India has come a long way in its pursuit of establishing mechanisms for electronic commerce and government. This development highlights the critical need for the government to establish a strong legislative structure for regulating the IT industry. In recent years, the term "global village" has become more common due in large part to the ways in which the information technology sector has altered communication infrastructure throughout the globe, particularly in India. Although this has helped bring people together from all walks of life, it has also made it hard for governments to safeguard sensitive data, which has given rise to a host of previously unanticipated problems stemming from illegal behaviour. The fundamental goal of the Information Technology Act was, thus, to set new norms for the control of human behaviour inside the virtual world of cyberspace.

Over some period of time, various new types of crimes began to be committed in this online realm. These crimes may be simply broken down into the categories described in the following way.

1. When a user makes unlawful use of the internet, they are engaging in the practice of cyber-squatting. In most cases, this is accomplished by registering a domain name that has the appearance of being identical to the name of a prominent or well-known domain, business, or brand. The person who commits the offence is called a squatter, and the name that is squatted is the name that the perpetrator uses. The cybersquatter was successful in registering the squatted domain name, giving them the first mover advantage and the ability to acquire legal rights to the domain name. The cyber squatter will then make a demand for payment from the proprietor of the well-known brand in exchange for the squatted domain, and in the event that the proprietor declines to purchase the domain, the cyber squatter will be granted the legal right to prevent the proprietor from making use of such names. These kinds of operations violate intellectual property laws, and in India, they also violate something called the "Uniform Domain Name Dispute Resolution Policy."

2. Barry Collin, a research fellow at the California Centre for Security and Intelligence, is credited with first using the phrase "cyber terrorism." According to him, the confluence of terrorism and cybernetics is included in what is meant by the term "cyber terrorism." Mark Politt, a special agent with the FBI, was the one who came up with the definition of cyber terrorism as a premeditated, politically motivated attack against computer systems, information, computer programmes, and data that amounts to violence against non-combatant targets and is carried out by clandestine agents or sub-national groups. In 2002, multiple messages relating to the Kashmir problem were aired on several notable websites in India. The crime, which was said to have been conducted by Pakistani Hackers led by one Doctor Naikar, marked India's first encounter with cyber terrorism strikes. The website of the Central Bureau of Investigation (CBI) was hacked by Pakistan Cyber Army in April 2010.
3. Theft of data happens when an unauthorised individual obtains information that is of a confidential nature and is prohibited from being disclosed to the general public by either stealing it or purchasing it via illicit means. The Information Technology Act of 2000 has provisions for dealing with offences of this kind under sections 43, 43A, and 66. The offence is covered under Section 43, whereas Section 43A and Section 66 deal with the penalties that may be imposed for similar offences. Even in the case of Syed Assifuddin and Others v. The State of Andhra Pradesh and Others, section 66 was cited as an applicable legal provision.
4. Hacking is an offence that covers a much wider scope, and one must be aware that it is one of those offences that may be done with a relatively low level of difficulty. In general, the term "hacking" refers to the illegal use of any computer or electronic device, information, or any other sort of data accessing or sharing devices, programmes, or the like. [6]Because hacking is such a broad category of criminal activity, it is possible that it includes using another person's email address without the permission of the owner of that email address in situations where the owner of that email address inadvertently kept that email address in logged in mode on a device. In India, hacking offences represent the most rapidly expanding category of cybercrime. Even the website of the Ministry of Defense, as well as the website of Jadavpur University and a great number of other significant websites, have been hacked on occasion. Under Section 66(2) of the IT Act, hacking has been treated as an offence; however, the word "hacking" has been substituted with the phrase "Computer related Offences" thanks to the Amendment Act of 2008. On the other

[6] Pavan Duggal, Text Book on Cyber Law (Universal Law Publishing Pvt. Ltd.,2013)

hand, any hacking done with a malicious or guilty intention for an illegal purpose will lead to unethical hacking, and Section 66(2) deals with unethical hacking. At the same time, we must also acknowledge that hacking can be categorised into ethical and unethical hacking. Ethical hacking means hacking with the permission of the owner of the concerned system in order to identify the possible vulnerabilities in the such system against future unethical hackings. Unethical hacking means hacking without

5. Web jacking is the process by which an unauthorised third party unlawfully seizes control of a website from its legitimate owner by cracking the website's password and then begins changing the material that is hosted on the website. The true owner of the website loses all control over it as a result of the forcible taking away of custody of the website. In the Indian legal system, offences of this kind are dealt with according to Section 65 of the IT Act, 2000.
6. It's common knowledge that bullying involves intimidating or threatening another person. Cyberbullying is defined as the practise of intimidating or threatening another person via the use of electronic means. The term "cyber bullying" refers to the intentional infliction of repeated injury via the use of electronic equipment such as mobile phones, personal computers, and other similar gadgets. According to the findings of the Global Youth Online Behavior Survey that was carried out by Microsoft in 2011, India ranked third in terms of cyber bullying, behind China and Singapore. It was estimated that approximately 53% of children were bullied online at some point during their time spent using various online platforms. Even though such offences may be brought within the purview of Section 66 and the criminal provisions of Section 43 of the Information Technology Act of 2000, Indian law has not provided a formal definition for cyberbullying.
7. Cyberstalking occurs when an individual engages in stalker behaviour while using a computer or mobile device. Stalking is defined broadly in the Indian Criminal Code as the persistent and intentional following of a person with the intent to harm them. Cyberstalking is a kind of stalking that takes place online. 114 This may not seem like a big deal at first, but it might end up violating people's privacy, which is a fundamental right under Article 21 of India's constitution[7]. While Indian law does not have a specific provision for dealing with cyberstalking, Section 72 of the Information Technology Act addresses the same issues. Section 354D of the Indian Penal Code now makes it illegal to engage in internet stalking, according to the Criminal Law (Amendment) Act of 2013. Nevertheless, this provision of the code only applies to male offenders and exclusively

[7] Roger W. Smith, “Cybercrime - A Clear and Present Danger: The CEO's Guide to Cyber Security” Create Space Independent Publishing Platform; 1 edition (21 June 2014)

protects female victims. Because of the potential for ambiguity in applying a gender-neutral interpretation to the crime of cyberstalking, it is essential that we go to Section 72 of the IT Act.

8. The term "phishing" refers to the practice of sending bogus emails to an individual with the goal of collecting sensitive information such as a credit card number, bank account information, ATM PIN, etc. Such crimes in India will be handled in accordance with the country's normal fraud laws.
9. Some actions, when carried out without the owner's or caretaker's consent, are considered criminal offences under Section 43 of the IT Act of 2000. These include, but are not limited to, the following: stealing data from such systems without authorization; exposing such systems or networks to viruses or any other kind of contaminations; damaging such systems digitally or physically; causing any sort of disruptions in the working of a computer system; preventing access to the system by someone who is legally entitled to access it; aiding and abetting offences with respect to any such computer systems; causing inadvertent damage to such systems; and causing inadvertent However, this Section only recognizes cyber-crimes involving digital and physical assaults on a computer, which only covers a limited subset of the many types of cyber-crimes that might cause harm to a computer system. Although Section 66 allows for a maximum sentence of 3 years in jail for similar offences, this Section establishes monetary penalties for their commission. [8]
10. For publishing obscene materials, the maximum penalty under Section 67 of the IT Act 2000 is three years in prison and a fine of up to Rs. 5 lakhs; for subsequent convictions, the maximum penalties increase to five years in prison and a fine of up to Rs. 10 lakhs. However, the most important difficulty with this Section is regarding the definition of Obscene materials, since legally any lascivious element that has the potential to cause excitement in any indiscriminate act is considered obscene Yet, each person has their own unique taste in lascivious material, so what gets one person excited may not get another. In addition, there are no cultural borders in internet, thus anything that might be considered culturally offensive in India may be perfectly acceptable elsewhere.in the US, for example. As everything posted online may be read by anybody, anytime, the veracity of the contents becomes questionable[9]. It is possible to dispute this Section on the basis that it violates Article 19 of the Indian Constitution, which would make it unconstitutional.

[8] Yatindra Singh (Justice), Cyber Laws (Universal Law Publishing Co. Pvt. Ltd.,2010)
[9] S. K. Bansal: Cyber Crimes (A. P. H. Publishing Corporation, Delhi) 2003

11. “Section 67 of the Information Technology Act of 2000” establishes a maximum punishment of three years in jail and a fine of up to Rs. 5 lakhs for the publication of obscene content; for consecutive convictions, the maximum penalties rise to five years in prison and a fine of up to Rs. 10 lakhs. Legally, every lascivious aspect that has the potential to produce excitement in any indiscriminate act is declared obscene. This presents the greatest challenge to this Section. Yet, each person has their own unique taste in lascivious material, so what gets one person excited may not get another. In addition, there are no cultural borders on the internet. Thus, anything that might be considered culturally offensive in India may be perfectly acceptable elsewhere. In the US, for example. As everything posted online may be read by anybody, anytime, the veracity of the contents becomes questionable. It is possible to dispute this Section on the basis that it violates Article 19 of the Indian Constitution, which would make it unconstitutional.[10]
12. In addition to these statutory provisions, the Indian government has also instituted a number of additional institutional initiatives to bring the country's information technology regulatory framework up to international norms. For instance, the “Information Security Management System (ISMS) Standard ISO” mandated that all government agencies follow its security policies and procedures. The government's cyber defences were a primary emphasis of the Information Security 5-Year Plan. In addition, many exercises were carried out to evaluate the level of readiness for dealing with cyber security incidents. Despite having a National Cyber Security Policy, India does not yet have a cyber certification body. Several government agencies undergo cyber security audits at varying intervals. Yet, the 5-year strategy on Information Security is moving forward at a glacial pace in terms of execution.[11]

4. JUDICIAL APPROACH

“The DPS MMS Scanal, or Avnish Rajaj v. State (NCT) of Delhi”[12], concerned the selling of a very sexually explicit MMS depicting a DPS female on the website baazee.com. Several copies of the MMS were sold, resulting in a substantial profit. “Although the website's CEO, Avnish Bajaj, was charged under Section 67 of the Information Technology Act for the publication and transmission of obscene materials, the defendant argued that he was not directly involved in the case and that, since the Section prohibited publication and transmission of obscene materials, his

[10] Roger W. Smith, “Cybercrime - A Clear and Present Danger: The CEO's Guide to Cyber Security” Create Space Independent Publishing Platform; 1 edition (21 June 2014)
[11] Yatindra Singh (Justice), Cyber Laws (Universal Law Publishing Co. Pvt. Ltd.,2010)
[12] (2005) 3 CompLJ 364 Del, 116 (2005) DLT 427, 2005 (79) DRJ 576

act did not amount to any of such activities and that the company took all reasonable steps to remove the video after 38 hours and that the delay of 38 hours was due to the intervention." The precedent-setting court agreed with his arguments and released him on bond, with conditions. "Syed Astifuddin v. The State of Andhra Pradesh"[13] was interference by Tata Indicom with a plan by Reliance Info COMM, in which Reliance provided a mobile device to the market at a low price, but the services under the scheme were exclusive to Reliance Info COMM. Tata Indicom personnel hacked into the company's mobile phones and began offering competing services, costing Reliance money. In court, Tata Indicom claimed that its staff had done nothing wrong under the IT Act. The court, however, rejected their claims and found that the cell phone is a "Computer" within the meaning of the Act's Section 2 and that their actions thus violated Section 65.

In the case "PR Transport Agency v. Union of India"[14], the issue was a contract between two parties that were made through email. The defendant signed the contract at first but later backed out, saying that technology made it impossible to keep the deal. The defendant said that the court didn't have the right to hear the case because the place where the email was sent was outside of the court's area of jurisdiction. The court didn't agree with the defendant's point of view, so it interpreted Section 13 of the IT Act, which has general rules about contracts made through email. It says that if a contract is made through email, the usual place of business should be taken into account when deciding which court has jurisdiction in case of a dispute. This is because emails can be received anywhere in the world, so taking into account where the emails were received would be very hard in practice.

5. CONCLUSION

As a result of the difficulty in interpreting the current legal requirements in light of the constantly evolving nature of cybercrime, the Indian Judiciary has had to deal with a significant backlog of cases. Of course, it's also important to note that cybercrime may originate from a variety of locations, not just inside one country. Such crimes may be performed at any time of day or night and from any place in the globe. In such cases, it is necessary to have a precise theory for choosing which bodies have the authority to rule on the matter according to the law. What is lawful in India may not be legal in other nations and vice versa; however, the internet respects no National borders, therefore cultural differences may also contribute to cybercrime. This is why a reliable

[13] 2006 (1) ALD Cri 96, 2005 CriLJ 4314.
[14] AIR 2006 All 23, 2006 (1) AWC 504.

certifying authority, working around the clock, is required to keep an eye on what people might find online.

Furthermore, international agreements must be reached for bringing uniformity in the legal regime since non uniformity may also lead to several cyber offences, for example, for opening a Facebook account one must be above 14 years of age, which means anybody can enter into contract with Facebook if he or she is above 14 years of age, whereas the Indian Contract Act requires the age of a party to a contract to be 18 years or older, and the state has not provided any restriction on who can enter into contracts. It's quite difficult to determine who is responsible for an offence when there are so many regulations that seem to contradict one another. Since cyberspace is an ever-evolving environment where new techniques of committing crimes and evading legal responsibilities will be invented repeatedly and within short amounts of time, laws must be made more particular and dynamic so that they can conform with the changing demands of the moment.