INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed JournalMulti Disciplinary
Peer Reviewed Edition :

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

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

ISSN: 2582-6433

Dr. Namita Jain

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 14th, 2019

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

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 methodology and teaching and learning.

ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS 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.

www.ijlra.com
Volume 2 Issue 7 | Aug 2023
ISSN: 2582-6433

A CRITICAL CHALLENGES IN CYBER SPACE AND LEGAL STUDY

AUTHORED BY: C DHANALAKSMI[1]
B. Com. LL.B (HONS), Undergraduate.
The Tamil Nadu Dr. Ambedkar Law University-SOEL.
E-MAIL ID: dhanalaksmi2003@gmail.com

ABSTRACT:

Any illicit action that uses a computer as its main tool for commission and theft is referred to as cybercrime. Cybercriminals or the hackers who want to generate money commit the majority, but not all, of cybercrime. Individuals or organisations can commit cybercrime. Some cybercriminals are well-organized, employ cutting-edge methods, and possess exceptional technical proficiency. Some hackers are amateurs. Cybercrimes will rise alongside technological advancements as technology plays a larger part in people's lives day by day. in the present paper we are going to see about the endless discussion with regarding the pros and cons of the cybercrime. There are many challenges in cyber space and related legal studies.

KEYWORDS: Cyber-Crime, Cyber-Hackers, Cyber-Criminals, Cyber-Laws.

INTRODUCTION:

Cybercrime refers to any illicit conduct that makes use of a computer as its main tool for theft and commission. Most, but not all, cybercrime is conducted by hackers or cybercriminals who are after financial gain. Cybercrime is committed by both individuals and groups. Some online criminals are well-organized, employ cutting-edge methods, and have extensive technical skills. Some hackers are newbies. As technology becomes more and more important in people's lives on a daily basis, cybercrimes will rise in tandem with these developments. Rarely does cybercrime want to harm computers for anything but financial gain. In today's scenario cybercrime is an emerging profession in the help of advanced technology and high-speed internet facility it has

[1] The Tamil Nadu Dr. Ambedkar Law University- SOEL
Email id: dhanalaksmi2003@gmail.com

ISSN: 2582-6433

created a great platform for the individual or groups to earn lots of money illegally. Cybercrime is simply defined as crimes that are directly related to computers and using computers.

OBJECTIVES:

- To know about the cybercrimes.
- To understand about the Cyber laws.
- To analyse about the challenges in cyber space.

CYBER LAWS:

Cyber law is the body of legislation that controls actions in cyberspace. The legislation governing the internet is known as cyber law. Cyberspace is a broad phrase that covers everything from computers and networks to software and data storage devices like hard drives and USB discs, as well as the internet, websites, emails, and even electrical gadgets like cell phones and ATMs. a location where E-messages exist while being sent from one computer to another computer but is not physically present. There are no physical borders in cyberspace. There are various sections in the law that penalise criminals who engage in cybercrimes. The Indian Penal Code, 1860 or the Information Technology Act, 2000 (IT Act, 2000) governs the offender's penalty. The following sections of the IT Act of 2000 and the IPC of 1860 are relevant:

- Where a person without the permission of owner or any other person in charge damages the computer.[2]
- Whoever, fraudulently or dishonestly makes use of e- signature, password or unique identity feature of another person shall be punished for 3 years or fine up to 1 lakh.[3]
- Whoever, by means of any communication device or computer resources cheat by personation shall be punished with 3 years or with fine.[4]
- Punishment for cheating by personation.[5]
- Making false document.[6]
- Punishment for forgery.[7]

[2] §.43 of IT Act,2000.
[3] §. 66(C) of IT Act, 2000.
[4] §. 66(D) of IT Act,2000.
[5] §. 419 of IPC, 1860.
[6] §. 464 of IPC,1860.
[7] §. 465 of IPC, 1860.

ISSN: 2582-6433

- Forgery for purpose of cheating.[8]
- Forgery for purpose of harming reputation.[9]

SOME OF THE CHALLENGES IN CYBER CRIMES:

IDENTITY THEFT:

The fraudulent practice of using another person's name and their personal details in order to obtain credit, loans etc. When a person uses another person's personal information, such as their name, identification number, credit card number, and so on, without that person's permission, they are committing fraud or another crime. Identity theft comes in four forms. They are as follows:

CRIMINAL IDENTITY THEFT: Criminal Identity theft is a type in which a thief pretends to be someone else when they are caught committing a crime. The thief makes use of the victim's personally identifying information, such as complete name, licence number, social security number, and other specifics, during an investigation or an arrest.

FINANCIAL IDENTITY THEFT: It can happen in a variety of ways, but often involves theft, online account hacking, or a data breach involving your account information giving someone else unlawful access to your bank cards or account information.

MEDICAL IDENTITY THEFT: When someone uses your personal information, such as your name, social security number, or Medicare number, to make false claims to Medicare and other health insurers without your consent, this is known as medical identity theft.

CHILDREN'S IDENTITY FRAUD: It can take many different forms. Despite the fact that the majority of children do not have a large number of bank accounts or lines of credit, scammers can nevertheless acquire a plethora of personal information about them. Social security numbers and login credentials for social media accounts are among the many things that thieves will steal. By use of stolen logins and passwords, they might be able to access other online accounts, and having access to social security numbers might allow them to open new accounts in your child's name.

DATA THEFT: If any person without the consent of the owner or any person who is in control of computer system. Data theft is the act of downloading copies of or extracting any data or information from a computer, including information saved on any removable storage medium.

[8] §. 468 of IPC,1860.
[9] §. 469 of IPC, 1860.

ISSN: 2582-6433

PHISHING: is a form of social engineering where criminals use deception to get their victims to expose personal information or download malicious software like ransomware. It is an offence where you are electronically impersonating or someone else for financial gain.

- Dragnet: They send bulk e-mails to the users and by clicking those mails their information will be taken.
- Rod & reel: In this people will be targeted and the fake id will be sent to them for acquiring their identity and the information related to them.
- Lobster pot: Targets the genuine website and the domain name will be taken and forged.

SOCIAL ENGINEERING: Criminals utilise social engineering to get in touch with customers directly, typically through phone or email. Often, they take on the role of a customer care representative to win your confidence and get the data they need. This data may contain your bank account number, employer name, and passwords. Before attempting to add you as a friend on social networking networks, cybercriminals will research you as much as they can online. If they get access to your account, they can start other accounts in your name or sell your information.

CYBERSTALKING: It is the practice of being followed by criminals on private social media accounts in order to get your private information and exploit it to their advantage. They have a variety of methods for gathering your information. They could be able to accomplish this by intercepting user passwords, obtaining personal data through social media, or disseminating phishing emails. This form of behaviour includes, but is not limited to, threats, defamation, slander, sexual harassment, and other attempts to intimidate, control, or otherwise harm the victim.

RANSOMWARE: Hacking into a user's data and preventing them from accessing it until a ransom is paid are known as ransomware assaults. Attacks by ransomware are crucial for all users, but they are even more crucial for organisations that need access to the data to carry out their regular operations. Yet, in the majority of ransomware assaults, the attackers try to demand additional money rather than releasing the data even after the ransom is paid.

BLOCKCHAIN AND CRYPTOCURRENCY ATTACKS:

While the ordinary internet user may not understand what blockchain and bitcoin are, companies value these technologies greatly. Because cyberattacks on these frameworks have the potential to harm customer’s data and corporate processes, they provide significant problems for enterprises

ISSN: 2582-6433

in terms of cyber security. These technologies are no longer in their infancy but have not yet developed to a sophisticated, secure phase. Companies must be aware of the security risks associated with these technologies and make sure that no openings exist for intrusion and exploitation.

KINDS OF CYBER CRIME

Cyber crime against the persons

When we look into cybercrime against a person it shall relate to offences like harassment which shall be through email sent through as a letters or an attachment. A very common way of online harassment is via social media platforms like facebook, instagram etc., crimes like cyber stalking shall take place by sending messages, videos or websites. Controlling of an individual computer and hacking it shall be completely performed through transfer of malware. By sendind messages, audio, symbols or videos to some other person's personal account in obscene language shall be claimed as online defamation. Cybercrimes shall be committed through cracking, SMS spoofing, fraud, cheating, child pornography, phishing etc.

Crimes against the person's property

Cyber crime performed on intellectual property consists of the rights of an individual such as design, Trademarks, software piracy etc. cyber crime against a persons personal property shall includes software piracy, cyber squatting, cyber vandalism, hacking through White-Hat hackers, Black-Hat hackers and Grey-Hat hackers.

Cyber crime against government

Cyber terrorism includes the hate email and hate website circulated throughout the world. Cyber terrorism is one of the hazardous crimes which endangers the integrity and unity of the nation. Other such crimes are cyber warfare, use of internet and terrorist, distribution of software's which are pirated, and position of unauthorized information.

Cyber crime against Society at large

It shall include child pornography, online gambling, cyber trafficking, financial crimes and forgery.

The above cited crimes are done against the society at large which shall cause complete harm to the cyberspace.

ISSN: 2582-6433

MAJOR CYBER CRIME CASES IN INDIA

Cosmos Bank cyber attack in Pune:

In 2018, Cosmos Bank which is situated in Pune had to suffer from a cyber attack which was a shock on banking sector of India where hackers siphoned off INR 94.42 crores of money from Cooperative Bank Limited in Pune.

UIDAI Aadhar application hacked:

There was a major data breach of personal record of 1.1 billion Indian Aadhar holder's. As per UIDAI, about 210 Indian Government's websites were hacked causing breach of data of 1.1 Billion Indians.

Official Maharashtra government website hacked In 2007, the official website of Maharashtra government got hacked where police of cyber crime division got involved in the case and tried to track down the hackers. In the result of hacking, the http:/www.maharashtragovernment.in website remained blocked for a day.

Official website of IRCTC hacked The official website of IRCTC got hacked which resulted the risk to put personal information of 1 crores of customer at stake.

SONY.SAMBANDH.COM CASE[10]:

India saw its first cybercrime conviction recently. It all began after a complaint was filed by Sony India Private Ltd, which runs a website called www.sony-sambandh.com, targeting Non Resident Indians. The website enables NRIs to send Sony products to their friends and relatives in India after they pay for it online. The company undertakes to deliver the products to the concerned recipients. In May 2002, someone logged onto the website under the identity of Barbara Campa and ordered a Sony Colour Television set and a cordless head phone. She gave her credit card number for payment and requested that the products be delivered to Arif Azim in Noida. The payment was duly cleared by the credit card agency and the transaction processed. After following the relevant procedures of due diligence and checking, the company delivered the items to Arif Azim. At the time of delivery, the company took digital photographs showing the delivery being accepted by Arif Azim. The transaction closed at that, but after one and a half months the credit card agency informed the company that this was an unauthorized transaction as the real owner had

[10] **CBI v. Arif Azim**

ISSN: 2582-6433

denied having made the purchase. The company lodged a complaint for online cheating at the Central Bureau of Investigation which registered a case under Section 418, 419 and 420 of the Indian Penal Code. The matter was investigated into and Arif Azim was arrested. Investigations revealed that Arif Azim, while working at a call centre in Noida gained access to the credit card number of an American national which he misused on the company's site.The CBI recovered the colour television and the cordless head phone. In this matter, the CBI had evidence to prove their case and so the accused admitted his guilt. The court convicted Arif Azim under Section 418, 419 and 420 of the Indian Penal Code — this being the first time that a cybercrime has been convicted. The court, however, felt that as the accused was a young boy of 24 years and a first-time convict, a lenient view needed to be taken. The court therefore released the accused on probation for one year. The judgment is of immense significance for the entire nation. Besides being the first conviction in a cybercrime matter, it has shown that the the Indian Penal Code can be effectively applied to certain categories of cyber crimes which are not covered under the Information Technology Act 2000. Secondly, a judgment of this sort sends out a clear message to all that the law cannot be taken for a ride.

YAHOO V. AKASH ARORA[11]:

It was one of the earliest examples of cybercrime in India. The defendant, Akash Arora, was accused of utilizing the trademark or domain name 'yahooindia.com,' and a permanent injunction was sought in this case.

THE BANK NSP CASE:

The Bank NSP case is the one where a management trainee of the bank was engaged to be married. The couple exchanged many emails using the company computers. After some time the two broke up and the girl created fraudulent email ids such as "indianbarassociations" and sent emails to the boy's foreign clients. She used the banks computer to do this. The boy's company lost a large number of clients and took the bank to court. The bank was held liable for the emails sent using the bank's system.

ANDHRA PRADESH TAX CASE:

Dubious tactics of a prominent businessman from Andhra Pradesh was exposed after officials of the department got hold of computers used by the accused person. The owner of a plastics firm was arrested and Rs 22 crore cash was recovered from his house by sleuths of the Vigilance

[11] 1999 PTC (19) 201 (Delhi)

ISSN: 2582-6433

Department. They sought an explanation from him regarding the unaccounted cash within 10 days. 11 The accused person submitted 6,000 vouchers to prove the legitimacy of trade and thought his offence would go undetected but after careful scrutiny of vouchers and contents of his computers it revealed that all of them were made after the raids were conducted. It later revealed that the accused was running five businesses under the guise of one company and used fake and computerised vouchers to show sales records and save tax.

STATE OF TAMIL NADU V. SUHAS KATTI[12]:

It was determined that the accused and the harasser had the same IP address. The proprietor of the Internet Café provided testimony against the defendants as an eyewitness. The Additional Chief Metropolitan Magistrate found the accused guilty of offences under Sections 469, 509 IPC, and Section 67 of the Information Technology Act, 2000 after relying on the expert witnesses and other evidence presented before the court.

SUGGESTIONS:

- Use Anti-virus software and keep the software updated.
- Use strong passwords
- Never ever open attachments in spam emails.
- Do not unnecessary open spam emails or untrusted websites.
- Unnecessary don't give personal information.
- Don't share the OTP or any other Passwords to anyone.

CONCLUSION:

Success in any field of human activity leads to crime that needs mechanisms to control it. Legal requirements should provide customers comfort, strengthen law enforcement, and prevent illegal activity. The legislation is strictly enforced, just how it should be. There are no longer any geographical, temporal, or social bounds to crime. Cyberspace leads to ethical, legal, and illegal wrongs. You may take easy precautions like using the most recent hardware and software for your digital requirements to safeguard your devices and data from cyber dangers. Also, you'll need to take sophisticated precautions like setting up a firewall to give an additional layer of security.

[12] CC No. 4680 of 2004

ISSN: 2582-6433

REFERENCE:

- Talwant Singh Addl. Distt. & Sessions Judge, Delhi, CYBER LAW & INFORMATION TECHNOLOGY, Success in any field of human activity leads to crime that need (delhidistrictcourts.nic.in).
- Majid Yar, Cyber Crime & Society, 2006.
- Classification Of Cyber Crimes (lawyersclubindia.com)
- **https://blog.ipleaders.in/critical-analysis-cybercrime-india/**
- 5 Types of Cyber Crime | Norwich University Online