AN OVERVIEW OF CYBER CRIME: A CRITICAL ANALYSIS WITH MODERN INDIAN SCENARIO IN 2024

Mr. Md Jiyauddin, Assistant Professor, School of Law, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Tamil Nadu, Chennai, imdjiyauddin@gmail.com
Dr. Sunita Banerjee, Assistant Professor, School of Law, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Tamil Nadu, Chennai, banerjeesunita93@gmail.com
Mr. Sandip Chanda, Assistant Professor, School of Law, Arka Jain University, Jamshedpur, Jharkhand, chanda.19.s2020@gmail.com

ABSTRACT:

Cybercrime is a modern form of criminal activity. According to the Information technologies Act, it is any illegal behaviour that occurs on or over computers, the internet, or other technologies. The most common crime that has a severe impact on modern India is cybercrime. In addition to generating massive damages to the government and society, the criminals are also quite good at hiding who they are. Technically proficient criminals use the internet to execute a variety of unlawful acts. According to a broader definition, cybercrime encompasses any unlawful conduct in which a computer or the internet is used as a tool, a target, or both. Although the term "cybercrime" is not defined in any act or legislation approved by the Indian Legislature, it may be construed judicially in some court rulings in India. The misuse of the increasing reliance on computers in modern life is the root cause of cybercrime, an unstoppable evil. The usage of computers and related technologies in daily life is expanding quickly and has become a necessity that makes life easier for users. It is an unbounded and incalculable medium.

Key-words: Common Crime, Unlawful Conduct, Indian Legislature, Judicially, Misuse and Technology.

INTRODUCTION:

Cybercrimes are offences that occur on the internet or through its medium. These cover a wide range of unlawful actions. Many criminal behaviours can be bundled together under the general term cybercrime. The anonymity of the internet has resulted to a number of unsettling behaviours taking place in cyberspace, which may allow offenders to engage in a variety of illegal actions known as cybercrimes. Since technology is used as a weapon in cybercrimes, the majority of those who perpetrate these crimes are technically proficient individuals who possess a deep comprehension of computer programs and the internet. Email spoofing, email bombing, cyber-terrorism, cyber-stalking, cyber-pornography, cyber-defamation, and others are some of the recently discovered cybercrimes. When done via the internet, several traditional crimes can also be classified as cybercrimes. For instance, the IPC, 1860, punishes theft, fraud, cheating, mischief, misrepresentation, intimidation, and so forth. Traditional crimes including drug trafficking, online gambling, financial fraud or forgery, cyber defamation, pornography, intellectual property crimes, cyberstalking, spoofing, etc. are typically modified by cybercrimes that use computers as a tool.

DEFINITION AND MEANING:

- *The Information Technology Act of 2000*: The precise definition of cybercrimes has not yet been established by any legislation or statute. Cybercrime is not defined in the IT Act of 2000 either. Cybercrimes, on the other hand, can be specifically defined as those types of crimes in which a computer is either the target of the crime, the subject of the crime, or both. Therefore, cybercrime encompasses any behaviour that involves a computer as a target, an instrumentality, or a method of committing more crimes.
- *S.T. Viswanathan, Prof*. He provided three potential definitions of cybercrimes, which are as follows:

a. Any unlawful activity when a computer is used as a tool or the aim of the crime, that is, any crime whose method or goal is to interfere with a computer's ability to function,
b. Any computer-related occurrence in which the offender intentionally made or might have made money while the victim suffered or could have incurred loss,
c. Any unlawful, immoral, or unapproved activity involving the automated processing and transfer of data is regarded as computer abuse.

- *The United Nations Congress on Cybercrime Prevention and Offender Treatment*: The UN Congress on Prevention of Cybercrime and Treatment of Offenders has established a global definition of cybercrime includes the two categories listed below:

i. Narrow sense: Cybercrimes as defined refer to any unlawful activity that attacks the security of computer systems and the data they handle and is carried out using electronic methods.
ii. In a broader sense, cybercrime encompasses all crimes involving computers and any unlawful activity carried out through or in connection with a computer system or network, including unlawful possession and the offering or dissemination of information via a computer system or network.

OBJECTIVE :

i. To analysis of characteristic of cybercrime.
ii. To find out criminal aspect of cybercrime.
iii. To discuss factors for contribute to cybercrime.
iv. To analysis modern Indian scenario on cybercrime.

SCOPE OF CYBERCRIME :

❖ Cybercrime is currently becoming more and more common, not just in India but globally as well. The prevalence of cybercrime is strongly correlated with a nation's degree of computer technology advancement. As per the United Nations research, over 50% of websites in the United States, Canada, and Europe have encountered security breaches and cyberterrorism threats, posing a significant challenge to law enforcement. Going to terror training is a new trend that has emerged in recent years among militants at order to educate recruits at cyber terrorist training camps, terrorists now use the internet as a primary teaching instrument.

❖ Speaking to the Internet security staff, Gabriel Weimann, a specialist in Internet and security who teaches at the University of Mainz in Germany and has spent almost ten years researching how militants use websites, stated that "websites and chat rooms used by militant Islamic Groups like Al-Qaida are not only used for dissemination of propaganda but also for terrorist education." Al-Qaida has released a useful website that demonstrates how to use firearms, conduct kidnappings, and create bombs out of fertilizer.

❖ The majority of nations in the world are already quite concerned about computer-related crime, and India is no different. Making the line between what is unlawful and what is immoral is the most important criterion to be taken into account when determining whether a certain computer-related action may be considered cybercrime. An action should only be considered a crime and the perpetrator should be prosecuted if it is genuinely unlawful. Consequently, criminal law must to be applied sparingly when deciding matters involving cyber law.

❖ Since there isn't a universally accepted definition of computer crime or cybercrime, legal professionals have been debating the terms "computer misuse" and "computer abuse," which are commonly used in relation to cybercrime. In this context, it is common practice to maintain that the two phrases have distinct meanings. The difference between accidental, careless, and purposeful computer system misuse must be made in the criminal legislation pertaining to cybercrime; the latter should be considered a crime rather than the former two. As a result of this distinction, misuse of a computer system should be considered criminal activity that is subject to legal penalties rather than behaviour that irritates or discomforts the computer user.

CHARACTERISTICS OF CYBERCRIME :

The word cyber, which signifies the science of communication and control over both humans and machines, is the root of the word cyber. Cyberspace is the next frontier for information and communication between people worldwide that is managed by machines. As a result, offences done online should be considered cybercrimes. Cybercrime, in its broadest definition, refers to any crime committed online, including hacking, terrorism, fraud, gambling, cyberstalking, cybertheft, cyberpornography, virus distribution, etc. Cybercrimes include both computer-related and computer-generated offences. It is the source of tension on a worldwide scale and is growing every second. Law enforcement organisations must thus be well-versed in the many types of cybercrime. However, the use of modern technology by criminals is nothing new. We must acknowledge that cybercrime is a relatively new phenomena with global political, social, and economic ramifications in this age of liberalisation and globalisation. National and international socioeconomic, political, and security systems are at risk from cybercrime. The primary traits of cybercrime are as follows:

i. **Low-risk, high-profit endeavour**: The most notable aspect of cybercrime is that it is very simple to perpetrate, challenging to identify, and even more difficult to prove. Basic computer skills and understanding allow cybercriminals to quickly destroy important databases, causing significant loss or harm to the crime's victims.

ii. **Victims' ignorance**: A victim of cybercrime frequently has no idea that it has happened because they lack the necessary skills and knowledge to operate the computer system.

iii. **No need for physical presence**: Cybercrime does not require the criminal to be physically present at the crime scene; it can be perpetrated from a great distance.

iv. **Insufficient technological proficiency among investigative agencies**: Investigators typically lack the high-tech skills necessary to discover cybercrimes.

v. **Victims do not disclose incidents**: For fear of negative publicity or the potential loss of public confidence, the party or organisation that has been the victim of cybercrime typically chooses not to disclose it to the authorities. The difficulty of detecting and controlling cybercrime is made worse by victims' unwillingness to come forward and lodge a police complaint.

vi. **No violence**: Cybercrime is not violent; rather, it is the result of mischief, greed, and taking advantage of the victim's vulnerability.

vii. **No national borders**: Because the Internet transcends national borders, cybercriminals are often able to evade legal action, making the issue of cybercrime more complicated.

viii. **Transparency and Anonymity**: The anonymity and openness of the computer network used to disseminate information make it simple and convenient for criminals to commit crimes without being recognised or recognised by the internet user who is the victim of their unlawful actions.

ix. **Lack of reliable evidence**: Since all information is sent electronically across a network system, if data is deleted, it cannot be recovered, and the criminal can avoid detection and conviction by destroying this one piece of evidence.

x. **Have more extensive effects**: The scope of cybercrime is broad enough to impact people's legal rights as well as their socioeconomic status.

xi. **People with specialised knowledge**: Since cybercrimes can only be carried out via technology, committing one requires a high level of proficiency with computers and the internet. Because the perpetrators of cybercrime are highly educated and possess a thorough grasp of how to use the internet, it is extremely challenging for law enforcement to apprehend them.

xii. **Territorial challenges**: In online, there are no territorial restrictions. A cybercriminal may quickly conduct crimes in another area of the world while sitting at any location. For instance, a hacker seated in India may compromise a system located in the United States.

CRIMINAL LIABILITY AND CYBERCRIME ASPECTS:

With a few notable exceptions, there are often two components to crime: mens rea and actus reus. Mens rea alone, for instance, is sufficient to impose criminal responsibility in conspiracy cases, whereas actus reus alone is sufficient to impose criminal liability in crimes against the state, such as fabrication of evidence, currency counterfeiting, white collar crime, etc. The fundamental tenet of criminal law is that no one can be found guilty of a crime unless the prosecution can demonstrate beyond a reasonable doubt that the defendant's actions were illegal, that he is accountable for them, and that he was in a certain state of mind when the crime was committed. As a result, actus reus without mens rea is not illegal.

Mens rea + actus reus = Crime
No Mens Rea + Actus Reus = No crime
Mens rea + no actus reus = No crime

According to J.C. Smith and B. Hogan, actus reus is a consequence of human behaviour that the law aims to stop. It is quite challenging to show both aspects of crime in the case of cybercrime.

ACTUS REUS :

Cybercrime has an extremely active and diverse actus reus. For instance, when someone starts using a computer with a keyboard and mouse, when someone tries to access data on another person's computer without that person's permission or consent, when someone tries to hack, flow viruses, commit cybercrime, and actually causes those acts, etc. In cyberspace, these are human behaviours or actus reus that the law aims to stop; in other words, these are actus reus of cybercrimes.

MENS REA:

Mens rea is yet another crucial component of cybercrime. Up until the 12th century, Smith and Hogan claim that actus reus was the sole way to hold someone accountable for harm without requiring evidence of mens rea or a guilty mental state. This idea has evolved in contemporary Common Law, where the commission of a crime and the application of punishment increasingly depend on having a guilty mentality. There is no definition or usage of mens rea in the Indian Penal Code, 1860. Nonetheless, mens rea is represented by the use of terms like purposefully, recklessly, knowingly, dishonestly, and fraudulently. As an example, when hackers hack, they are aware of or want to get unauthorised access, which is a cybercrime.

FACTORS THAT CONTRIBUTE TO CYBERCRIMES :

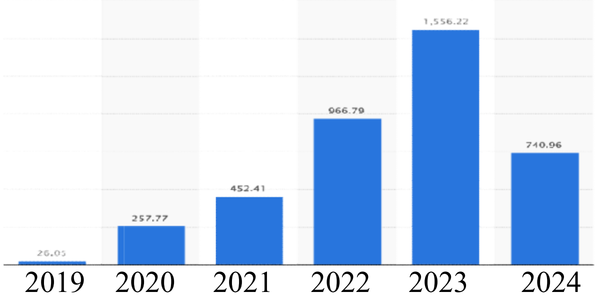
Professor H.L.A. Hart asserted in his seminal book, "The Concept of Law," that since people are susceptible to crimes and other illegal activities, laws are necessary to safeguard them from such behaviour. Applying the same example to cyberspace, computer systems are incredibly susceptible even if they are high-tech instruments. It is simple to utilise this technology to trick or take advantage of a person or his computer through unauthorised or unlawful access. Abuse of computer systems may have caused the victim's harm directly or indirectly. Because there is no infallible system in place to protect and shield innocent computer users from cybercrime, cybercriminals continue their illegal operations over networks without fear of being caught and placed on trial for their crimes. The following succinctly describes the factors that make computers susceptible to cybercrime:

1. **Large capacity for storing data**: The ability of the computer to store vast amounts of data in a comparatively little amount of space is one of its special features. In a CD-ROM, a tiny microprocessor computer chip can hold thousands of pages. There is sufficient room in this storage capacity to extract or extract information from visual or physical media considerably more easily. Even if the power is switched off, any data stored in ROM will not be affected. No matter what kind of ROM is used, the data contained within is non-volatile and will stay that way eternally until it is purposefully overwritten or wiped.

2. **Greater information accessibility**: The computer is an electrical device that uses sophisticated technology to do its tasks instead of human labour. Wider access to information resources across a vast and varied media is the biggest benefit of networking in the computer era. Networks are being used by an increasing number of businesses to make information freely accessible to their clients, employers, and other parties. This explains why, in the current digital era, networking and cyber activity are becoming more and more commonplace. The World Wide Web has made it possible to disseminate knowledge globally more quickly and affordably by creating new resources. It has produced a new environment for conversations, downloads, emails, and other activities. Everyone is now only a mouse click away from one another. Wider access to information, however, comes with drawbacks, such as the need to safeguard computer systems from unwanted access, which can happen not because of human mistake but rather because of intricate technological manipulations.
3. **Computer systems**: The complexity Operating systems, which are made up of millions of codes, are what the computers run on. Due to the fallibility of the human intellect, a mistake might occur at any point. These flaws and gaps are exploited by cybercriminals to get access to the computer system. These crooks, who take advantage of flaws in current operating systems and security equipment, are known as hackers. Because they take advantage of the intricacy of computer systems and are driven by personal revenge, sabotage, fraud, greed, or animosity towards the victim, hackers are the dreaded adversary of the Internet and general network security.
4. **Carelessness of network users**: Human behaviour is intimately linked to negligence. Consequently, it is quite likely that a user will make a mistake or be careless in securing the computer system, which might provide a cybercriminal the chance to obtain unlawful or unauthorised access to or control of the machinery. Interaction with a diverse group of computer users has revealed that they prioritise security, control, and access measures over regular software operation, which gives cybercriminals the opportunity to compromise systems and steal, alter, or destroy large amounts of data. This is especially true for large institutions like government offices, banks, and enterprises.
5. **Lack of proof or its disappearance**: Digital computer processing and network technologies have now supplanted the old ways of creating, storing, sending, and sharing information or records. How to gather and maintain evidence is the actual problem facing law enforcement and investigative organisations. In contrast to traditional offences, it is exceedingly challenging to gather enough proof of a cybercrime that would hold up in court and prove the accused person's guilt beyond a reasonable doubt. The anonymity offered by the Internet to cybercriminals encourages them to commit crimes without leaving any trace, and even if they do, it is rarely enough to persuade the authorities that a criminal case can be filed against them. The low conviction rate for cybercrimes indicates that the majority of cybercriminals obliterate evidence to avoid being found guilty. Due to the shortcomings of conventional evidence and criminal investigation techniques, a new techno-legal process known as cyber forensics has had to be adopted. Although forensic specialists are crucial in gathering and presenting admissible electronic evidence as well as conducting searches and seizing tangible evidence related to the cybercrime being investigated, there are still some grey areas that allow the cybercriminal to manipulate the evidence in order to deceive the investigating authorities.
6. **Uncertainty over jurisdiction**: Cybercrimes transcend national boundaries, making it difficult and illegitimate to enforce domestic laws, which are often based on geographic or territorial authority. Because cybercrimes are international in nature, they do not recognise geographical boundaries because they are perpetrated through the interconnectedness of internet networks. Because various countries have varied laws and procedures for dealing with cybercriminals, jurisdictional conflicts represent a severe danger to a country's ability to deal with these criminals. Frequently, a specific internet behaviour is considered illegal in one nation but not in

the one where the offender or victim resides, which makes it easy for the criminal to avoid punishment. The law enforcement agencies of each nation struggle greatly to combat cybercrimes and criminals using their own legal systems in the lack of a unified, globally accepted rule of law and procedure governing cybercrimes. Due to the lack of cyber jurisdiction in the nation looking into these offences, there are very few cyber cases that are reported and convictions are made. Additionally, the lack of clarity in the law enables cybercriminals to carry out their evil deeds without hindrance. The IT security company McAfee has disclosed a worldwide investigation into intentional intrusions or cyberattacks against non-profits, companies, and governments. The investigation, known as "Operation Shady RAT" a widely used acronym for remote access programs that let you access computers from a distance follows a string of cyberattacks against businesses over a five-year span in various geographic regions. Since the 14-page report became viral online, there has been a lot of conjecture regarding the attack's origin. Although it notes that the hacking of the World Anti-Doping Agency, the IOC, and the Asian and Western National Olympic Committees suggests that these assaults have a non-commercial motivation, the study itself does not identify the offender.

Number of cyber-crime cases registered by the Indian Cyber Crime Coordination Centre (I4C) in India from 2019 to 2024



Modern Indian scenario on cybercrime in 2024

NUMBER OF COMPLAINTS:

Between January and April 2024, more than 740,000 cybercrime complaints were recorded on the Ministry of Home Affairs' National Cybercrime Reporting Portal. According to the Indian Cyber Crime Coordination Centre (I4C), an average of 7,000 cybercrime complaints were reported per day in May 2024, a surge of 113.7% from 2021-2023 and 60.9% from 2022-2023, with 85% of them being financial online scams. This is an increase of 113.7% from 2021-2023 and 60.9% from 2022-2023.

FINANCIAL LOSSES:

According to data compiled by the Indian Cyber Crime Coordination Centre (I4C), a division of the Ministry of Home Affairs (MHA), India lost about Rs 11,333 crore to cyber fraud in the first nine months of 2024. In the first four months of 2024, Indians lost over ₹1,750 crore to cybercriminals.

CYBER FRAUD IN BANKING TRANSACTIONS:

India's rapid growth in online transactions has coincided with an unparalleled increase in cyber-crime. Between FY2020 and FY2024, 5,82,000 occurrences of cyber fraud resulted in a loss of ₹3,207 crore, as reported by the Reserve Bank of India in response to the authors' Right to Information application. With digital purchases expected to skyrocket again this festival season, this figure gains relevance. The fiscal year 2024 has been an unprecedented year for cyber fraud, exceeding the preceding three years in terms of both the number of occurrences and the money lost. The number of cyber fraud instances rose from 75,800 in FY 2023 to 2,92,800 in FY 2024. The amount lost increased from ₹421.4 crore in FY2023 to ₹2,054.6 crore in FY2024.

INVESTMENT SCAMS:

Cybercrime is quickly changing, with sophisticated schemes on the increase in India by 2024. Criminals use digital platforms and psychological weaknesses to defraud naïve individuals in anything from bogus investment schemes to fear-based scams. These crimes result in large financial losses and weaken faith in digital systems that are becoming increasingly important in everyday life. Investment frauds caused a loss of Rs 222 crore in 62,687 complaints.

DIGITAL ARREST SCAMS ON RISE:

"Digital arrest" schemes took advantage of people's anxiety and ignorance by imitating law enforcement officials. Victims received phone calls, emails, or texts accusing them of involvement in crimes such as money laundering, drug trafficking, and tax avoidance. Fraudsters demanded rapid payment of fines or bribes to avoid legal action or arrest, and frequently threatened to block bank accounts. Scammers misled victims into downloading monitoring software and demanding 24-hour surveillance of the attacker.

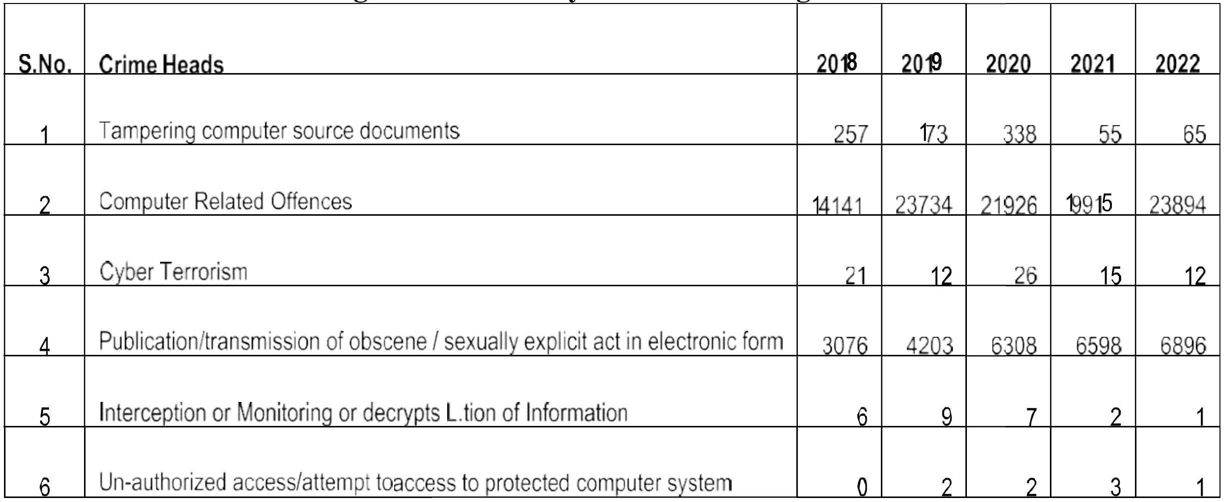
Scammers often utilised bogus arrest warrants or faked government seals to boost their legitimacy. This swindle disproportionately impacted professionals and retirees. With developments in spoofing and phishing tactics, fraudsters used panic to take money quickly. Stock trading frauds accounted for the most losses, at Rs 4,636 crore from 2,28,094 complaints. Investment-based scams resulted in losses of Rs 3,216 crore from 1,00,360 complaints, while "digital arrest" frauds cost Rs 1,616 crore across 63,481 cases.

DATING APPS:

The I4C, formed by the Ministry of Home Affairs, provides a framework for law enforcement authorities to combat cybercrime. The huge increase in reported instances is seen from 2019 to 2024, with 26,049 complaints registered in 2019, 257,777 in 2020, 452,414 in 2021, 966,790 in 2022, 1,556,218 in 2023, and 740,957 in the first four months of 2024 alone.

The majority of victims fell victim to online investment fraud, gambling applications, algorithm manipulation, illicit loan apps, sextortion, and OTP scams. In 2023, the I4C recorded more over 100,000 cases of investment fraud. Digital arrests resulted in a loss of Rs 120 crore over 4,599 instances in the first four months of 2024. Trading scams accounted for 20,043 incidents, resulting in a loss of Rs 1,420 crore to hackers throughout the same time. According to I4C statistics, investment frauds resulted in a loss of Rs 222 crore over 62,687 complaints, while dating apps generated losses of Rs 13.23 crore across 1,725 complaints. The entire financial toll caused by hackers on Indians between January and April 2024 was Rs 176 crore.

Crime Heads-wise Cases Registered under Cyber Crime during 2018-2022



S.No.	Crime Heads	2018	2019	2020	2021	2022
1	Tampering computer source documents	257	173	338	55	65
2	Computer Related Offences	14141	23734	21926	19915	23894
3	Cyber Terrorism	21	12	26	15	12
4	Publication/transmission of obscene / sexually explicit act in electronic form	3076	4203	6308	6598	6896
5	Interception or Monitoring or decrypts L.tion of Information	6	9	7	2	1
6	Un-authorized access/attempt toaccess to protected computer system	0	2	2	3	1

7	Abetment to Commit Offences	1	0	1	7	4
8	Attempt to Commit Offences	13	14	18	5	18
9	Other Sections ofITAct	980	2699	1017	827	1017
A	**Total Offences underI.T.Act**	**18495**	**30846**	**29643**	**27427**	**31908**
10	Abetment of Suicide (Online)	7	7	10	10	24
11	Cyber Stalking/Bullying of Women/Children	739	771	872	1176	1471
12	Data theft	106	282	98	170	97
13	Fraud	3353	6229	10395	14007	17470
14	Cheating	2051	3367	4480	6343	10509
15	Forgery	260	511	582	198	224
16	Defamation/Morphing	18	19	51	31	61
17	Fake Profile	78	85	149	123	157
18	Counterfeiting	2	5	9	2	2
19	Cyber Blackmailing/Threatening	223	362	303	689	696
20	Fake News on Social Media	97	188	578	179	230
21	Other Offences	1713	1974	2674	2456	2857
B	**Total Offences under IPC**	**8647**	**13800**	**20201**	**25384**	**33798**
22	Gambling Act (Online Gambling)	20	22	63	27	37
23	Lotteries Act (Online Lotteries)	2	9	26	4	6
24	Copy Right Act	62	34	49	32	27
25	Trade Marks Act	0	1	5	1	14
26	Other SLL Crimes	22	23	48	99	103
C	**Total Offences under SLL**	**106**	**89**	**191**	**163**	**187**
	Total Cyber Crimes (A+B+C)	**27248**	**44735**	**50035**	**52974**	**65893**

CONCLUSION:

These days, one of the most important issues facing nations worldwide is cybercrime. includes violating security measures like passwords and privacy, as well as gaining unauthorised access to information for anybody using the Internet. Cybercrime, which refers to robbery carried out using a computer or the Internet, includes cyber theft. The government is creating more stringent regulations to safeguard people's interests and shield them from any unfavourable incidents on the Internet in response to the rise in cyber security fraud and crimes. Furthermore, in order to ensure data protection and privacy, stronger regulations pertaining to the protection of confidential personal data have been developed in the hands of intermediaries and service providers corporate bodies. Although the nation's legislative body has passed a number of legislations, the government still has the most difficult issue in combating cybercrime. Additionally, the Indian legal system lacks technical procedures, therefore even though the substantive criminal law is adequate, it cannot be implemented in India because of these procedural shortcomings. The fundamental issue with cybercrime is that there are certain ways that the internet may be abused; the criminals are the ones who always abuse it in new ways, thus the legal system is unable to fulfil their needs. In addition, because cybercrime is global in nature, international cooperation was necessary. Just passing legislation is insufficient; international cooperation is necessary for cyber law to function. Although the Information Technology conduct of 2000 and all of its connected legislation have provisions pertaining to transnational jurisdiction, they may only be put into effect after every nation in the world has acknowledged the conduct as a criminal and permitted the proceedings on that basis.

REFERENCES :

1. Pavan, D. (2016). *Textbook On Cyber Law*. 2nd edn., Universal Law Publishing.
2. Ashok, K. J. (2019). *CYBER LAW Information Technology Act*. ASCENT Publication.
3. Vaishnavi, G. (2022). An Analysis Of Cybercrime Investigation And Surveillance. *Indian Journal of Law and Legal Research*. Retrieved from https://www.ijllr.com/post/an-analysis-of-cybercrime-investigation-and-surveillance#:~:text=The%20NCRB%20has%20reported%20the,nations%20for%20cyber%2Dcrime%20victims.
4. Singh, P. D., & Loura, D. (2021). Cyber Security in Civil Aviation: Current Trends. *Dehradun Law Review*. 13(1), 95-105.
5. Vakul Sharma, I. T. (2011). *Information Technology Law and Practice*. New Delhi: Universal law publishing.
6. Rani, S. (2022). CYBER CRIMES IN INDIA: A CRITICAL ANALYSIS. *International Journal of Mechanical Engineering*. 7(6), 304-312.
7. Vithalani, N.P. (2023). CYBER CRIMES AND LAW IN INDIA: A CRITICAL ANALYSIS. *International Journal of Creative Research Thoughts*. 11(8), 942-947.
8. Adam, M. B. & Tamar, B. (2019). Introduction: new directions in cybercrime research. *Journal of Crime and Justice*. 42(5), 495-499.
9. Animesh, S., Roshmi, S, & Amlan J, (2017). A brief study on Cyber Crime and Cyber Law's of India. *International Research Journal of Engineering and Technology*. 4(6), 231-237.
10. Nidhi N. *Cyber Crime In India: An Overview*. Retrieved from https://www.legalserviceindia.com/legal/article-4998-cyber-crime-in-india-an-overview.html
11. *Facing the Cybercrime Problem Head-On*. Retrieved from https://www.sciencedirect.com/topics/psychology/cybercrime
12. Dipanshu, R. (2024). *EMERGENCE OF CYBERCRIME IN DIGITAL SOCIETIES CHALLENGES, REGULATIONS AND ETHICAL CONSIDERATIONS*. Retrieved from https://articles.manupatra.com/article-details/EMERGENCE-OF-CYBERCRIME-IN-DIGITAL-SOCIETIES-CHALLENGES-REGULATIONS-AND-ETHICAL-CONSIDERATIONS
13. *Cybercrime*. Retrieved from https://www.britannica.com/topic/cybercrime

14. Ahmad, S. (2020). Cyber Crime in India: An Empirical Study. *International Journal of Scientific & Engineering Research. 11(*5), 690-694.
15. Mokha, A.K. (2017).A Study on Awareness of Cyber Crime and Security. *Research J. Humanities and Social Sciences.* 8(4), 459-464. doi: 10.5958/2321-5828.2017.00067.5
16. Sunidhi, K. (2021). *Prevention of Cyber Crimes in India: A Comparative Study.* Retrieved from http://hdl.handle.net/10603/379851
17. Divakar, S. *A Study on Cyber Crime and its Related Laws in India.* Retrieved from https://journal.esrgroups.org/jes/article/view/4466
18. *What is cybercrime? How to protect yourself.* Retrieved from https://www.kaspersky.com/resource-center/threats/what-is-cybercrime
19. Telecom, (2024). NCRB report shows sharp increase in Cyber Crime cases in states, Metros; overall dip in IPC cases registered in 2022. Retrieved from https://telecom.economictimes.indiatimes.com/news/internet/ncrb-report-shows-sharp-increase-in-cyber-crime-cases-in-states-metros-overall-dip-in-ipc-cases-registered-in-2022/105720313
20. GOVERNMENT OF INDIA MINISTRY OF HOME AFFAIRS. (2024). Retrieved from https://www.mha.gov.in/MHA1/Par2017/pdfs/par2024-pdfs/RS27112024/226.pdf