International Research Journal of Commerce and Law
Volume 13 Issue 01, Jan 2025 ISSN: 2349-705X Impact Factor: 8.843
Journal Homepage: http://ijmr.net.in,
Email: irjmss@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal

CYBER CRIME & PROTECTION RIGHTS OF CHILDREN IN DIGITAL ERA: A SOCIO LEGAL STUDY

Rupashree Choudhuary[1],

Prof.(Dr.) N.C. Patnaik[2]

Abstract :

Cybercrime is a cross-border crime as it has no boundary. Criminals are using the internet medium to conduct unlawful and illegal activities. We are living in the digital era. Technological advancement, which have impact on human life in various ways. In India rapid digitization and penetration of smart phones for expanded a digital space and exposed the marginalized children towards cyber exploitation. In recent part, there has been a concerned rise in cybercrime against the children. Since the time of Pandemic (Covid-19) children are spending more time on online games, entertainment and for other activities, which has exposed the children to wide range of cybercrime. In the rent past a worrying trend of increasing rate of cybercrime against the children has been observed, as per the statics of NCRB-2022. The report states that in the year 2021 total 1376 numbers of cybercrime were reported against the children, but in the year 2022, surprisingly the reported trends increased by almost 32% i.e., up to 1823 numbers of crimes were reported. It is, thus, evident that the cyber crime against the children in our country has a tendency of rapid growth. Further, it is pertinent to mention here that the NCRB data indicates that in the last few years crime against children has increased to a significant percentage in online and offline mode like Maharashtra: 12.8%, M.P.: 12.6%, U.P.: 11.5%, Rajasthan: 5.8%, West Bengal: 5% are the top five States in the country. In India, as a legislative measure to deal with the cybercrime, Law has been enacted for protecting the children like IT Act, 2000, POCSO Act, 2012, Bharatiya Nyaya Sanhita, 2023, which provides the legal framework to deal with the cyber attackers. Hence, my research work is meant for preparing a parameter strategy to mitigate the risk in cyber space and to ensure the rights of children in digital era.

Key Words: Cyber Crime, Child, Rights .Technology and protection.

[1] . Research Scholar, Law, Berhampur University ,Berhampur,Odisha.
[2] . Professor cum Principal, Lingaraj Law College, A Constituent College of Berhampur University, Odisha.

1. Introduction:

The Internet is now an indispensable part of the daily life styles. It is evolved into a formidable system that has influenced business, commerce and day-to-day life of every individual. Because of this only, there is a rapid expansion of different types of online crime. Cybercrime has emerged because of rapid expansion of the data highway. Of course, the government has begun to educate police officials about "cyber-security" "Mobile surveillance", "tracing anonymous emails", etc.A child in the twenty-first century spends many hours each day online playing video games and surfing the internet. On the internet, they encounter a variety of risks. Because due to lack of expertise, they cannot assess the potential risks and threats associated with the usage of digital technology and the internet. Sometimes, children may reveal their confidential information and exposed themselves to unwanted consequences in a variety of ways. Hence, they can fall under the situation of cyber security dangers like "social-engineering," "cyber-bullying," "hacking," "viruses," "cyber stalking," and other things through search engines, online marketing, and social networking websites. As we know child pornography is a punishable offence in India, which is prohibited under statutory law like Information Technology Act, 2000, Protection of Children from Sexual Offences Act, 2012 and Indian Penal Code, 1860, Juvenile Justice (Care and Protection of Children) Act, 2015 and Commission for Protection of Child Rights Act, 2000.

Inventions, discovery & Technologies not only widen scientific horizon but also pose new challenges for the legal jurisprudence. Nature has gifted human beings with mind and brain power which distinguished them from other creatures and make man superior among other living creatures of universe. Cyber law is the law governing computer & internet technology. Digital technologies have made dramatic changes in our routine life style. Today, almost every human need is facilitated by cyber space, including education, shopping, banking, govt. schemes, online medical consultations etc. However, its relevance is not limited to providing services. The platform has given voice to the socially marginalized communities.[1]Social media has become a platform where ideas are discussed and debated, policies are welcomed or criticized. Science is a

branch of knowledge and a study of natural phenomena by way of observations, identifications, descriptions, experimentations & investigations. Law is a living process which changes according to the changes in the society, science, ethics and so on. The legal system should imbibe developments and advances as long as they do not violate fundamental legal principles. The Criminal Justice System should be based on equitable principles. Due to modern advancement of science & technology, the modus operandi of committing crimes has been totally changed. The criminals are committing crimes with the latest invention of science & technology. So, for prevention of such types of crimes, the present methods of crime detection are not sufficient. Today, normal criminal behaviour has been transformed into electronic criminal behaviour relating to Cyber Crime. As the world becomes increasingly digital and interconnected, the question arises, "What is cyber law?" The massive influence and usage of Cyber space has not only attracted potential users but also criminals. Apart from its various capabilities of making life easier, it has also created situations of terror. From WHO to Cognizant to MSMEs and individuals, cyber criminals have left no one.[2] Another study indicated an increase of two- thirds in cybercrime in lock downed India.[3] Such situations demand the need of strong measures by government, to regulate the cyber space and keep such activities at bay. At its core, cyber law serves as the guiding force behind our online interactions, ensuring they remain secure, ethical, and within legal parameters. Right from safeguarding personal data to setting standards for online behavior, cyber law touches every aspect of our online experiences. With rapid advancements in technology and our increasing reliance on the internet, understanding cyber law becomes more paramount. So, with that in mind, let's embark on this enlightening journey together.

Cyber Law often referred to as the digital code of conduct, is a specialized field of law. It addresses the legal challenges and intricacies associated with the internet, digital technologies, and electronic elements. Essentially, it encompasses a broad spectrum, from computer software and hardware to information systems. Cyber law is designed to safeguard and govern our online interactions, ensuring that they remain within legal boundaries.

But what is cyber law, and what makes it so pivotal in our contemporary world? Our

[1]Bedeley, "Giving Voice to the Voiceless: The Use of Digital Technologies by Marginalized Groups", 20 *Communications of the Association for Information System*, 2019, 556-559.

reliance on technology has grown manifold, especially since we use some sort of technology every single day. This increased dependence has opened the doors to a plethora of cyber threats. Armed with sophisticated tools, cybercriminals are constantly on the prowl, seeking vulnerabilities to exploit. This makes the digital space a potential minefield where a single misstep can lead to significant damage.

For professionals in cyber security and those specializing in cyber law, understanding its nuances is indispensable. In fact, their expertise plays a pivotal role in deciphering the complex web of digital rights, responsibilities, and potential liabilities.

The rise in cybercrimes is alarming. From data breaches to identity theft, the digital world is rife with dangers. This surge underscores the necessity for a robust legal framework. Such a framework deters potential cyber criminals and provides a clear path for redressal for victims of cybercrimes.

Types of cybercrime against the children:

(i) Child pornography;
(ii) Cyber-stalking;
(iii) Cyber-bullying
(iv) Defamative
(v) Hacking
(vi) Identity theft
(vii) Online child trafficking
(viii) Violation of privacy
(ix) Violation of human rights

Similarly new online games are also a challenging concept. As a preventive measure of cybercrime against the children like (i) blue-wave online games challenges (ii) suicide cases of teenagers; (iii) pass-out challenges; (iv) the salt and ice challenges; (v) the fire challenges; (vi) the cutting challenges. Similarly, in the recent cases related to internet, the Bois Locker Room case is also an important aspect for protection of children from cybercrime. Besides the above,

there are also various legislations namely:

I. Data Protection Laws

Data protection laws ensure that users' personal and sensitive data are meticulously shielded from unauthorized breaches and misuse. These laws, in essence, are the backbone of our online privacy, safety, and dignity.

II. Copyright and Intellectual Property Laws

When creators ask, "What is cyber law doing for my digital creations?" the answer lies in these laws. They are meticulously crafted to protect the rights of creators. This ensures that their digital innovations remain safeguarded from unauthorized use or replication, providing a haven for creativity.

III. E-commerce Laws

For those navigating the bustling lanes of online business, e-commerce laws serve as guiding lights. They meticulously regulate online transactions, ensuring they're not only secure but also transparent, thus fostering trust among all parties involved.

IV. Cybercrime Laws

The digital realm, while offering endless possibilities, also harbors shadows of cybercriminal activities. They act as guardians by penalizing activities ranging from malicious hacking to online harassment to keep the digital space safe.

V. Digital Signature Laws

The digital signature laws validate the authenticity of digital signatures in electronic documents. In essence, they are the pillars that uphold the trustworthiness of digital agreements and contracts.

VI. Privacy Laws

Every individual cherishes their privacy. Recognizing this universal truth, these laws

ensure that the sanctity of users' online privacy remains inviolable. This allows the average person to explore the digital world with peace of mind.

VII. Domain Name Laws

As the internet continues its exponential growth, domain names have become prime digital real estate. Furthermore, these laws regulate the registration and usage of domain names, ensuring a harmonious digital environment devoid of conflicts.

VIII. Cyber security Laws

National security is paramount, and these laws recognize the potential cyber threats to critical infrastructures. These laws help fortify the digital space against any threat from malicious actors.

IX. Freedom of Expression Laws

The digital age has a democratized voice, allowing everyone to share their perspectives. Therefore, these laws ensure that this voice remains unshackled, free from undue censorship or backlash.

X. Consumer Protection Laws

Online consumers, often wondering what cyber law does for them, find their answer in these laws. Furthermore, they are the shields that protect consumers, ensuring they receive genuine products and services free from digital deception.

At present, there exist two statutes for cybercrimes. One is the Indian Penal code, and second is the Information Technology Act. Generally, any crime which is punishable under IPC, if involves a substantial use of Cyber space would be a cyber-crime punishable under IPC. It includesStalking (Section 354D), Forgery(Section 473), Fabricating false evidence(Section 192),CriminalIntimidation(Section503),Defamation(Section499),Cheating(Section420), Extortion (Section 383), Obscenity (Section 292) etc.

In the Information Technology Act, 2000, Chapter IX and Chapter XI, enumerates specific cybercrimes, their corresponding punishments and power of adjudication. It includes Identity theft (Section 66C), Cheating by personation (Section 66D), Violation of privacy (Section 66E),CyberTerrorism(Section66F),CyberObscenity (Section67),ChildPornography(Section 67B) etc.

Forthepurposesofcrimeprevention,theActprovidesenormouspowerstotheCentralorState Government to order interception or decryption of any information through any computer resource[1]. Also, the government has power to authorise monitor and collect traffic data or information through any computer resource for cyber security.[2]

While the Indian Criminal Justice System does offer some degree of protection against cybercrimes, its effectiveness in adequately addressing this growing menace is widely acknowledged to be insufficient. Despite legislative measures such as the Information Technology Act, 2000, and subsequent amendments, the system faces numerous challenges that impede its ability to effectively tackle cybercrimes.

- **Lack of Specialized Expertise**: Investigating and prosecuting cybercrime requires specialized knowledge and skills in digital forensics, cybersecurity, and technology law. However, many law enforcement agencies lack the necessary resources and expertise to handle complex cyber investigations effectively.
- **Jurisdictional Challenges:** Cybercrime is often transnational in nature, with perpetratorsoperatingacrossinternationalbordersto evadedetectionandprosecution. Jurisdictionalissuesarisewhencrimesarecommittedincyberspace,makingitdifficult to determine which laws apply and which authorities have jurisdiction over the case.
- **Inadequate Legal Frameworks:** While the Information Technology Act, 2000, providesalegalframeworkforaddressingcybercrime,gapsandloopholesinthe legislation hinder its effectiveness.The law may not adequately cover emerging forms of cyber threats, legislationhinderitseffectiveness.Thelawmaynot adequatelycoveremerging forms

[1]The InformationTechnology Act,2000,Sec69,No. 21,Actsof Parliament,2000(India).

ofcyberthreats,leavinglawenforcementagenciesandprosecutorsstrugglingtoadapt to new challenges.

- **Low Cybercrime Reporting Rates:** Many cybercrime victims hesitate to report incidents to law enforcement due to concerns about privacy, reputation, and the perceived ineffectiveness of the criminal justice system. As a result, a significant number of cybercrimes go unreported, making it difficult to assess the true extent of the problem and allocate resources accordingly.
- **Limited International Cooperation:** Cooperation and coordination among law enforcementagenciesatthenationalandinternationallevelsareessentialforcombating cybercrime effectively. However, bureaucratic hurdles, differences in legal systems, anddiplomatictensionsoftenimpedecollaborationefforts,allowingcybercriminalsto operate with impunity across borders.

Cybercrime poses a significant threat to individuals, businesses, and governments globally, withtheIndiancriminaljusticesystemfacingnumerouschallengesinaddressingthiscomplex issue. To effectively combat cybercrime, there is an urgent need for enhanced collaboration between law enforcement agencies, investment in specialized training and technology, and continuous adaptation of legal frameworks to keep pace with evolving cyber threats. Only throughconcertedeffortsandcoordinatedactioncanwemitigatetheriskposedbycybercrime and safeguard the integrity of cyberspace for future generations.

2. Aimsand Objectives:

Theprimaryaimofthisresearchistocomprehensivelyanalysescybercrime against childrenanditslegal challenges within the criminal justice system. The objectives include:

- To study the emerging growth of cybercrime against the children
- To strengthen and protection regarding cybercrime in I.T. Law, 2000, POCSO Act, 2012 and Indian Penal Code, 1860;
- Juvenile Justice (Care & Protection of Children) Act, 2015;

- Commission for Protection of Child Rights Act, 2000;
- I.T. (Intermediary Guidelines and Digital Media Ethics Code) Rule-2021
- The enforcement problems of legislative measures to minimize cybercrime against the children;
- Role of human rights in comparison for protection of cybercrime.
- The role of Government for protection of cybercrime.
- Toprovide a comprehensive understanding of cybercrimeanditsvarious manifestations within the digital landscape.
- To analyse the existing legal frameworks governing cybercrime at both national and international levels.
- Toidentifythechallengesfacedbylawenforcementagenciesininvestigatingand prosecuting cybercriminals.
- To assess the effectiveness of current legal measures in addressing cyber threats and protecting individuals and organizations.
- Toexaminetheimpactofcybercrimeonsociety,economy,andnationalsecurity.
- Toexploretheroleoftechnologyinbothfacilitatingandcombating cybercrime.
- To evaluate the adequacy of resources, training, and infrastructure available to law enforcement agencies for combating cyber threats.
- Toinvestigatetheroleofpublicawarenessandeducationinpreventingcybercrimeand promoting cybersecurity best practices.
- To propose recommendations for enhancing the legal response to cybercrime and improving coordination among law enforcement agencies.
- To contribute to the ongoing discourse on cybercrime and inform policymakers, legal professionals,andthegeneralpublicabouttheevolvingnatureofcyberthreatsandthe challenges

they pose to the criminal justice system.

3. ResearchProblem:

There is no doubt internet has made our life much easier and more convenient. We can use internet to communicate with people around the word. By using internet and making new friends we can know different cultures, informations and data for our academic purpose. However, despite a glaring benefits and positive aspects, the internet is its both dark and bright faces too. One of this dark side that must be addressed is the problem of cybercrime against the children. Children now-a-days addicted to internet, most preferably after Covid-19 and they visited internet on a daily basis. No doubt this is one of the greatest threats posed to children. Internet has provided an easy medium to children to gain access to different cybercrimes in their day-to-day lives.

Therefore, cybercrime against children has emerged as a pervasive and multifaceted threat in the digital age, posing significantchallengestolawenforcementagenciesandthecriminaljusticesystemworldwide. Despite the proliferation of cyber threats, the effectiveness of legal frameworks in addressing cybercrime within the criminal justice system remains a subject of debate and concern. This research aims to investigate the efficacy of existing legal measures in combating cybercrime and the challenges faced by law enforcement agencies in enforcing these laws effectively.

The primary research problem revolves around the adequacy of current legal frameworks in addressingtheevolvingnatureofcyberthreatsandprovidingeffectiveremediesforvictimsof cybercrime. While legislative efforts such as the Information Technology Act, 2000, and its subsequent amendments seek to criminalize and deter cyber offenses, gaps and loopholes in thelegislationoftenhindertheirimplementationandenforcement.Moreover,thetransnational nature of cybercrime poses jurisdictional challenges, making it difficult to prosecute perpetrators operating across international borders.

THREATS OR CHALLENGES AGAINST THE CHILDREN UNDER CYBERCRIME:

(i) **Grooming on the internet**: Cyber grooming is a cyberthreat to children worldwide, not just in India. This is essentially a threat in which a person attempts to develop an emotional connection with a child through cyber means. Individuals participate in this through a variety of cyber channels, including social media and online gaming websites. The person poses as a child, and the children eventually believe him. As the child's trust in the imposter grows, the imposter gains the ability to exploit and exploit the child.

(ii) **Bullying on the internet**: Cyberbullying is another big element of today's cyber threats. It is essentially the act of harassing other children by using obscene or abusive language. This can be accomplished by sending children harmful content. However, it has the potential to harm a child's self-esteem. It's critical to realise that if a child's cyberbullying isn't caught early on, it can have far-reaching consequences. Some of the ramifications are detrimental to a child's mental and emotional well-being. As a result, their development may be significantly hampered.

(iii) **Online transaction fraud**: Despite the fact that the vast majority of children lack personal bank accounts. They do, however, frequently use their family accounts, particularly their parents' accounts, for all online transactions such as shopping and gaming. Criminals use a variety of deceptive tactics as calling to offer you benefits while using a false identity to steal money from your account.

(iv) **Gaming on the internet**: Online gaming has now become a common part of a child's daily routine. Furthermore, due to technological advancements and accessibility, online gaming has evolved into a way for people from all over the world to share their thoughts while playing. In some ways, it has morphed into a form of social media. However, when connecting with people through online gaming, there is a tendency to be careless, which can lead to harm. Furthermore, while installing the software, there is a risk of being infected with spam and viruses. This can lead to cyberbullying via

foul language, invasion of children's privacy due to the large amount of personal information that is uploaded and can be misused, and online transaction fraud.

(v) **E-mail scam**: Today, no work or activity would be possible without communication. It's indeed a leader in today's society. The primary mode of communication is the mail, and as such, it has become an essential part of society. To participate in any online activity, whether gaming or social media, we usually need to use email. When the data of such companies is stolen, the email addresses are made available to a large number of unauthorised people. As a result, anyone in the country can send emails with viruses, malware, and bugs in them.

4. Hypothesis:

(i) The changing scenario and concept of cybercrime against the children is an umbrella under which many illegal activities may be grouped together which needs and effective measures in the cyber space.

(ii) The impact of various offences which take place on using the medium of internet and social media on cybercrime against the children need to be an effective mode of technological solution.

(iii) Judiciary in India has to encourage and support for speedy and cost-effective remedy in cybercrime against the children.

(iv) Lacunae and Loopholes in the existing legislative framework in India to be a strong approach with a statutory and constitutional mandate to combat cybercrime against the children.

(v) The current legal framework and law enforcement strategies are inadequate in combating cybercrime against the childreneffectively.

(vi) Therapidevolutionoftechnologyandtheglobalnatureofcyberthreats necessitate a more robust and adaptive approach to law enforcement and legal intervention.

(vii) Mandatory age verification for social media platforms will decrease the number of children exposed to harmful online content.

(viii) The use of AI powered to detect and remove harmful content will reduce children's exposure to online pornography.

5. LiteratureReview:

Theliteraturereviewwillexamineexistingresearchandscholarlyarticlesoncybercrime against children,legal challenges, and the criminal justice response in India. It will explore the various types of cybercrime, including hacking, identity theft and online child trafficking, etc. Additionally, the review will analyse the evolution of cyber laws at both domestic and national levels, highlighting their strengths and weaknesses in addressing modern cyber threats against children.

Chandradeep Singh Samrao[1]–In this book, the author explores the historical perspective, origins,andproliferationofcybercrimes,offeringinsightsintotheiruniquecharacteristicsand themethodsemployedtoperpetratevarioustypesofcybercrimes against children.Itdelvesintothenuances of verification and the necessity of proving intent in cybercrimes, particularly focusing on offenses outlined in the Information Technology Act, 2000. Additionally, the book outlines national efforts to combat cybercrime against children, providing a comprehensive overview of human right in this regard.

DeepthiArivunithi[2]–Thestudyanalysesthevarioustypesofcybercrimes against childrenandotherinvasions ofprivacywhicharenotmadepunishableundertheITAct,fore.g.,Spamming.Italsodiscussed the issue of interception of calls as an invasion of privacy in digital communication and lays down that it is only justified if done by a procedure established by law. The study concludes by emphasizing the need for awareness among people of the nitty gritty of cyber space and concrete steps to protect their privacy in the virtual world.

Devashish Bharuka[3] – Thestudyanalyses thebridginggapbetweenthecybercrimes against children andthe traditional crimes under IPC. It focuses on how the crime in the cyber world poses new problems of interpretation before Investigators, Judges, Lawyers who are unfamiliar with the new technology and finds it hard to prosecute the cyber criminals. For e.g. The procedure of collecting evidence in the cyber world becomes complicated since it involves the use of data

trails.Also, thestudy findsthatnon-inclusion ofcertaincrimesundertheIT Act makes it less effective for curbing the menace of cyber offences. The study concludes by emphasizing the needofpositive,technicallyinclined,innovativeandenthusiasticcyberforcefortacklingsuch crimes.

Dr. M. Dasgupta[1]– The author offers a comprehensive examination of cybercrime against children with a particularemphasisonitsprevalenceandimpactinIndia.Thebookmeticulouslyexploresthe natureandelementsofcybercrime,providinginsightsintothetheoriesofcriminalliabilityand behavior in cyberspace. The book traces the history and evolution of cybercrime, providing readers with a contextual understanding of its emergence as a significant societal challenge. Dasgupta examines major cybercrimes prevalent in contemporary times, including cyber hacking, cyber fraud, cyber pornography, and cyber terrorism, offering insights into their underlying mechanisms and implications.The author critically examines the varying approaches to cybercrime regulation and enforcement across different jurisdictions, highlighting the challenges and opportunities for collaboration in combating transnational cyber threats against children.

Dr.S.V.JogaRao[2]–Theauthoroffersanextensiveexplorationofthecomplexlandscapeof cybercrimes against children and their evolving trends. The book delves deeply into the nature of criminal conductincyberspaceandexaminestheprofoundimpactofcybercrimeonsocietyatlarge. One of the key strengths of the book lies in its comprehensive coverage of different facets of informationtechnology,includingemergingissuesandimplicationsforlegalregulations.

Dr. Talat Fatima[3]– In this book, the author provides a comprehensive examination of the background,nature,andtaxonomyofcybercrime,addressingthechallengesinherentin defining elusive cybercrimes. Drawing on perspectives from scholars like Ian Walden, D. S. Wall, and the European Convention of 2001, Fatima offers nuanced insights into the multifacetednatureofcybercrimes against children.Asignificantfocusofthebookisonthelegalcomplexities involved in combating cybercrime. Fatima explores jurisdictional issues, examining the challenges of enforcing laws across borders in the digital realm. Additionally, she delves into the enforceability issues arising from divergent legal frameworks and international treaties.

[1]Dr. M.Dasgupta,*Cybercrime in India,* (Eastern Law House,Kolkata, 2016).

[2]Dr.S.V.JogaRao, *Cyber Crimes &InformationTechnologyLaw*,(WadhwaandCompany,Nagpur,1st Edition, 2007).

[3]Dr.Talat Fatima,*Cybercrimes*,(EasternBookCompany,Lucknow,2016).

Moreover,thebookshedslightonevidentiaryissuescrucialtotheprosecutionofcybercrimes. Fatimaanalysestheintricaciesofgatheringandpresentingelectronicevidence,consideringthe unique challenges posed by digital investigations.

Dr. Vishwanath Paranjape[1]– The author presents a thorough examination of cybercrime against children andtheirimpactoninternetusers.Thebookdiscussesthelegalprotectionsavailabletovictims, the nature and scope of cybercrime, including Intellectual Property Related cybercrimes, and the tools used by cyber-criminals. It also offers a global perspective on cybercrime, highlightingitsprevalenceandimpactacrossdifferentregions.Overall,thebookisavaluable resource for understanding and addressing the challenges of cybercrimes against children in today's digital landscape.

Luv Solanki & Dhaval Chudasama[2]– The author highlights the dynamic nature of the Internet, which, whileoffering immensebenefits,alsoattracts variousformsof cybercrime. It discusses India's proactive approach in combating cybercrimes through the enactment of the Information Technology Act, as well as similar efforts undertaken by other nations globally. However, despite these legislative measures, there is a growing recognition of the need for international cooperation and the formulation of global laws to effectively address cyber threats.Thetextemphasizesthatwhilecyberlawsaimtopreventsuchcrimesthroughpunitive measures,significanteffortsarestillrequiredtoadequatelyaddressthecomplexitiesofmodern cybercrime landscapes.

NirKshetri[3]–Thestudyretracesthecausesofcybercrimesindevelopingcountrieslike India and found that economic and institutional factors like lack of resources, unawareness among thelawenforcementcommunity,non-reportingofcrimescontributestotheoverallincreasein the growth of offences in the cyber space. Also, it highlights various offences which have not been included in the IT Act which can have devastating effect on people's privacy. For e.g., Phishing,CyberStalking,etc.Thestudyconcludesbyadvocatingontheneedofhavingstrong regulatory institutions.

Olukunle Oladipupo Amoo & Akoh Atadoga et. al.[1]**–** The research paper provides an

[1] Dr.VishwanathParanjape, *LegalDimensions ofCyber CrimesandPreventive Laws*,(CentralLawAgency, Allahabad, 2010).

[2] Luv Solanki&DhavalChudasama,"CyberCrimes andChallengesFacedby CriminalJustice System", 7.1, *IJISSE*,2021.

[3] NirKshetri,"DiffusionandEffects ofCyber-Crime inDevelopingEconomies",31(7)*THIRDWORLDQ*.2010,1057-

overviewofthecomplexlegallandscapesurroundingcybercrimeanditsimpactonthecriminal justice system. It highlights the challenges posed by cybercrimes in today's digital era, emphasizing the need for a comprehensive understanding of contemporary legal issues. Key aspects covered include jurisdictional complexities, technological advancements, and the global nature of cyber threats. The analysis underscores the importance of international collaboration and standardization of legal norms to address these challenges effectively. Furthermore, it discusses the dynamic nature of cybercrimes and the urgency for legal frameworks to adapt accordingly. Additionally, the paper addresses concerns regarding individual privacy and civil liberties in cybercrime investigations, advocating for a balanced approach. Overall, it emphasizes the necessity of a cohesive international legal framework to combat cybercrime and ensure justice in the digital age.

RRevathi[2]**–**Thestudyexploresthevariousfacetsofprivacyinthemajorlegalsystemsofthe world. It included issues of Bugging, Telephone Tapping, Interception, threats to confidentiality of communications, etc. which are common to most nations including India. Also, it also contemplates the great danger of privacy being abused in the cyber space by describing the continuous violation of copyright in the cyber world. The study concludes by advocating for a Right to anonymity in cyber space.

S.S. Singh[3] **–** The study focuses on the inherent conflict between Right to privacy and data protection.Theconvergenceoftechnologieshasenhancedtheprobabilityofabuseofprivacy. Instanceslikeinterceptionofemails,phonecallsareshowntobehugeviolationsofinformation privacy of an individual. The study concludes by depicting the inefficiency of the IT Act and stresses the need of a separate legislation on data protection

Steven Furnell[4]**–** The author provides a comprehensive exploration of the significance and far-reaching impact of cybercrime on modern society. The book meticulously examines an array of cybercrimes, shedding light on issues surroundinghackers, hacker culture, and the proliferation of malware in its diverse forms. Furnell'sanalysis extends to the various manifestations of malware, offering insights into their functionalities and potential consequences for individuals and organizations alike. By delving into these intricacies, the book underscores the complexity

[1] OlukunleOladipupoAmoo,AkonAtadegaet.al.,"Thelegallandscapeofcybercrime:Areviewofcontemporary issues in the criminal justice system",2(2), *WJARR*, 2024,205–217

[2] R.Revathi,"PervasiveTechnology,InvasivePrivacyandLucrativePiracy –ACritique",51(3)IJIL(2009),369. https://www.jstor.org/stable/43953454

and ever-evolving nature of cyber threats in the digital age.Moreover,thebookservesasacalltoaction,drawingattentiontothepressingcybercrime problems that confront society. Through thoughtful reflection on the implications of cybercrime, Furnell prompts readers to consider its broader societal ramifications and the urgency of addressing thesechallenges. Overall, the book provides acompelling examination of cybercrime's multifaceted nature and its profound implications for society as a whole. It serves as a valuable resource for policymakers, cybersecurity professionals, and anyone concerned with safeguarding the integrity of the information society against malicious cyber activities.

Vivek Sood[1] **–** The author provides an in-depth analysis of various aspects of cybercrimes against children in thedigitalage. Notably, thebook delves into thecontemporary relevanceof pornography and addresses the evolving role and responsibility of intermediaries in regulating onlinecontent.

Theauthorextensivelycoversawiderangeofcybercrimes,includingtheplantingofcomputer viruses and contaminants, forgery in digital signatures, dissemination of xenophobic content through blogs, and data-related crimes. Additionally, the book explores complex issues such as hacking, cyber stalking, and cyber terrorism, shedding light on their implications in the moderndigitallandscape.Asignificantportionofthebookisdedicatedtodiscussingelectronic evidence and the investigative processes involved in addressingcybercrimes.Italsoexamines whether India should accede to international cybercrime conventions, providing insights into the implications and considerations involved. Furthermore, the book critically examines the intersectionofprivacyandsecurityconcernswithintheframeworkofSection69oftheITAct, 2000. This section empowers certain government agencies to intercept, monitor, or decrypt data for investigative purposes. Sood's analysis prompts readers to contemplate the balance between privacy rights and the need for effective cybercrime prevention and investigation.

6. ResearchGap:

Despite the abundance of literatureon cybercrime, there is a gap in understanding the specific legal challenge within the Indian criminal justice system to prevent cybercrime against children. While many studies focus on technical aspects or legislative frameworks, few delve

[1]VivekSood,*Nabhi'sCyberCrimesElectronicEvidenceandInvestigationsLegalIssues*,(NabhiPublication, Delhi, 2010).

into the practical implementation of cyber laws against the cybercrime against children and their impact on law enforcement practices.

Cyber security gaps are the flaws in the cyber security.

- Password management
- Data encryption and key management
- Endpoint protection (anti-virus, anti-malware) – endpoint security doesn't stop at just anti-virus software but also includes other products such as firewalls and HIPS (host intrusion prevention systems). This is because there are so many different types of attacks; one product cannot protect against all of them. Therefore, it's important to use multiple products from different vendors to cover all angles of attack.
- Application safe listing only allows specific applications on your network rather than letting anything run/open by default; this helps prevent malicious code from running, further compromising your network.
- Patch management - keeping all software updated with the latest patches and hot fixes keeps hackers out by making it harder for them to exploit known vulnerabilities within applications or operating systems; however, keep in mind not every patch will fix everything, so don't rely solely on patches being released by vendors.

This research aims to bridge this gap by providing a comprehensive analysis of cybercrime against children from a legal perspective.

7. Research Methodology:

This research study is based on both doctrinal and non-doctrinal research methods. The study also based on analytical study. The data for this research study is based on secondary sources i.e., reference section, library, newspaper, journal and internet site, etc.

The secondary data has been collected from various published sources like bare act, ministry of electronics and information technology, online journals and other related websites. These data has been classified into cybercrimes and cyber law in India. Research methodology is a way to systematically solve the research problem. It will be understood as a science of studying

how research is done scientifically. The study highlights the methodology and process used to conduct the present research, the objectives and the procedures of the study. When appropriately conducted, research reduces any kind of ambiguity and brings clarity to the result and thus becomes helpful for the study to plan its goals and objectives accordingly. The Researcher through this study highlights the shortcomings of Cyber legislation in India and suggests the measure to prevent and control cyber-crime against children effectively. The researcher will specifically deal with cyber-crime against children in the Indian Scenario and suggested measures to control the cyber-crime against children in India. It also suggests measures to improve the existing law and things that need to be done to prepare the policy and judiciary to control cyber-crime against children.

8. The purpose of the study:

The purpose of the study was to conduct an examination into the impact of cyber involvement on victims of child exploitation. It is also to find out better way to prevent children from falling victim of cybercrime. The children being engaged on the internet and on the online platform, there is every apprehension of prey of cybercrime. Although internet has its positive side, but the negative side is now more disadvantage than the positive side. We know that every child has the fundamental human rights to take advantage of this invention that has come to humanity positively. However, the dark side of this invention is exposing children to internet cybercrime. Therefore, significant of the State was to have a better understanding and to enhance a strong statutory approach of law to prevent a child from falling victims of cybercrime.

9. Conclusion & Suggestions:

There are various factors that makes children more vulnerable of the cybercrime. Today we are living in the age of technology where everyone is dependent on technologies. Now we can say that technology has a material in the development of human life. Life is very easy after the rapid growth and development of the technologies. But at the same time, we pay a huge loss. In the recent year, number of cybercrimes has a big threat to the human life. So, it is very necessary to make strict laws to regulate technologies slowly but surely.

There is constant proliferation of new digital technologies and digitization of almost all financial and non-financial transaction taking place all over the world. With the increase of usage of the ICT and internet there are possibilities of technological threats. The protection of the mankind in general and children in particular is at most important for the Government. In India IT Act, 2000 to deal with cybercrimes plays an important role in the protection from cybercrimes along with the IPC, 1860, Juvenile Justice (Care & Protection of Children) Act, 2015 and POCSO Act, 2012, etc. There is a greater need for international harmonizing efforts, coordination and cooperation among various nations. More Focus Should Be Given on E-commerce, online contract, IPR, e-governance etc.

Suggestions

(i) Educate children about digital technology at school in order to make them informed and assure safety in digital world.

(ii) To enhance the digital skill competency and literacy teachers.

(iii) The parents, teachers and guardians can be good digital role models for children.

(iv) To prevent and block the websites, networks, social networking sites and services from distributing and disseminating of materials while abusive and offensive for children.

(v) More steps should be taken by Government of India as well as WCRB to make more effective towards policy measures for protection of children from cybercrime.

(vi) Constitutional provisions under 7th schedule i.e., the entertainment machinery towards prevention of cybercrime against children should be more stringent.

(vii) IT (Intermediary Guidelines and Digital Media Ethics Code) Rule, 2021 should be more effective.

(viii) National cybercrime protecting portal (**www.cybercrime.gov.in**) has been established to help the public to report instant cyber crime should be more expansion to help filing online cyber complaint in addition to toll free number 1930.

(ix) Stricter legal framework for protection of children from sexual offences should be included in the POCSO Act, 2012.

(x) National Commission for the Protection of Child Rights (NCPCR) should be given statutory power to exercise its duties towards protection of offences against children.

Bibliography

(1) *Sheikh Danish – "Rainbow of possibilities" (The Hindu dated 31/08/2017, Page-9)*

(2) *Kamil Mariyam – "How Privacy Stacks Up" (The Hindu dated 28/08/2018, Page-8)*

(3) *Apar Gupta & Ujwala Uppaluri – "A Fundamental Error" (The Hindu dated 01/08/2018, Page-8)*

(4) *"Long way to go for Digital India" – The Hindu dated 02/03/2018, Page-9*

(5) *Ujwala Uppaluri – "Naming a Right" (The Hindu dated 02/03/2018, Page-9)*

(6) *"Protection of Personal Data – A Right" - The Hindu dated 22/07/2017, Page-1*

(7) *Sukumar Arun Mohan – "Recognize the technology constraints" – The Hindu dated 07/12/2017, Page-9*

(8) *Mandira Moddie – "Protecting our Data" – The Hindu dated 23/03/2018, Page-9*

(9) *"Children under attack" – The Hindu dated 15/03/2017, Page-11*

(10) *The Hindu dated 26/05/2022, Page-10*

(11) *The Hindu dated 15/03/2017, page-11*

(12) *The Hindu dated 15/06/2022, Page-10*

(13) *Vakul Sharma & Sheema Sharma – "Information Technology Law and Practice" – 6th Edition, 2018 Universal Law Publication Co. (Lexis Nexis)*

(14) *Nandan Kamath – "Law Relating to Computers, Internet and E-Commerce" Universal Law Publication 5th Edition (2016)*

(15) *Prof. S.N.Mishra – Indian Penal Code as amended by Criminal Law (Amendment) Act, 2018 – 22nd Edition 2020 Central Law Publication, Allahabad*

(16) *Dr. Avtar Singh – "Principles of the Law of Evidence" 20th Edition 2013, Central Law Publication*

(17) *M.P. Jain – Indian Constitutional Law 6th Edition 2012 (Lexis Nexis) Nagpur*

(18) *J.N. Pandey – Constitutional Law of India, 44th Edition 2007 Central Law Agency, Allahabad*

(19) *Immoral Traffic Prevention Act, 1956*

(20) *Indian Penal Code, 1860, Code of Criminal Procedure, 1973 and Information Technology Act, 2000*

(21) *https://indiankanoon.org/doc/4439440*

(22) *https://www.lawyersclubindia.com/articles/classification-of-cybercrimes-1484.asp*

(23) *Bhagtani.H.T. (2017) – Cyber Crimes & Cyber Security, Mumbai: Himalaya Publication House Pvt. Ltd.*

(24) *https://www.dailypioneer.com/2019/state-editiorals-digital-literacy-initiative-forgovt-schools-kids.html.*

(25) *Madan Kumari – "Cyber Crime and Children in Digital Era" International journey at scientific research in Science & Technology ISS No.2395601, Vol.8, Issue-I, P.No.151/160, Jan-Feb, 2021.*