CYBER CRIME, REGULATION AND SECURITY

CONTEMPORARY ISSUES AND CHALLENGES

EDITED BY
PROF. DR. PRADEEP KULSHRESTHA
PROF. DR. ANITA SINGH
DR. RITU GAUTAM

THE LAW BRIGADE
PUBLISHERS

CYBER CRIME, REGULATION AND SECURITY: CONTEMPORARY ISSUES AND CHALLENGES

EDITED BY:
PROF. DR. PRADEEP KULSHRESTHA, DEAN, SCHOOL OF LAW, SHARDA UNIVERSITY
PROF. DR. ANITA SINGH, PROFESSOR, SCHOOL OF LAW, SHARDA UNIVERSITY
DR. RITU GAUTAM, ASSISTANT PROFESSOR, SCHOOL OF LAW, SHARDA UNIVERSITY

PUBLISHED BY
THE LAW BRIGADE PUBLISHERS,
LIBERTATEM MEDIA PVT. LTD.
F104, ANAND SQUARE, TRAGAD IOC ROAD,
CHANDKHEDA, AHMEDABAD 382470
WEBSITE: HTTPS://BOOKS.THELAWBRIGADE.COM

1ST EDITION
ISBN: 978-81-956533-0-0

NOTE: DUE CARE AND DILIGENCE HAS BEEN TAKEN WHILE EDITING AND PUBLISHING THIS BOOK. NEITHER THE AUTHOR NOR THE PUBLISHER OF THE BOOK HOLDS ANY RESPONSIBILITY FOR ANY MISTAKE THAT MAY HAVE INADVERTENTLY CREPT IN.
THE PUBLISHER SHALL NOT BE LIABLE FOR ANY DIRECT, CONSEQUENTIAL, OR INCIDENTAL DAMAGES ARISING OUT OF THE USE OF THIS BOOK.

ABOUT THE CONFERENCE

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

Cyber Crimes are risky for different organizations and people networking on the internet. It poses a great challenge and threat for individuals as well as for society. The objective of the National Conference on Cyber Crime Security and Regulations – 2022 was to examine the emerging cybercrime security and regulation issues and trends in the current scenario. This conference was multidisciplinary in nature and dealt with debatable and relevant issues that the world is facing in cyberspace in the current scenario.

This conference provided a platform to legal professionals, academic researchers and consultants an opportunity to share their experiences and ideas through panel discussion and paper presentations across the country and witnessed nearly 150 participations.

Thank You!

School of Law, Sharda University, Noida

CONTENT

1

CYBER CRIMES AGAINST MARGINALISED AND VULNERABLE GROUPS IN INDIA

KEYWORDS

CYBER CRIME, SECURITY AND REGULATION, INFORMATION TECHNOLOGY ACT, SENIOR CITIZENS AND MARGINALISED GROUPS, DIGITAL INCLUSION

CHAPTER ONE

CYBER CRIMES AGAINST MARGINALISED AND VULNERABLE GROUPS IN INDIA

AUTHORS

ADITI SRIVASTAVA, RESEARCH SCHOLAR, SCHOOL OF LAW, SHARDA UNIVERSITY, INDIA

MR. AVINASH KRISHNA GOSWAMI, RESEARCH SCHOLAR, SCHOOL OF LAW, SHARDA UNIVERSITY, INDIA

DR RITU GAUTAM, ASSISTANT PROFESSOR, SCHOOL OF LAW, SHARDA UNIVERSITY, INDIA

ABSTRACT

Cyber space and its regulation are a fast-developing arena, having multidisciplinary disciplinary approach to tackle the innovation, technological developments and cybercrimes emerging from interactions in cyberspace. The potential victims are those marginalised group who need socio legal support to become aware, prevent themselves from falling prey to such crimes and getting speedy justice, remedy and taken seriously that cybercrime perpetrated against them is as valid and graver as any traditional crime. This exploratory research paper presents a critical analysis of challenges faced by all the stakeholders, jurisprudence of nature of such cybercrimes perpetrated against Senior Citizens just as Women and Children were experiencing since emergence of Information Communication Technology, what new principles or prepositions are found, in order to fully elucidate the scope. nature and extent of these acts which constitute cyber crimes, methods employed by cybercriminals to reflect their intents, objective to victimise Marginalised group, cyber law framework in Indian scenario, judicial recommendation and environment to provide speedy justice, community support for prevention and counselling for victims, efforts needed for digital literacy of the Senior Adults to have a digitally inclusive society which is able to avail the benefits of Digital Media, Information Communication Technology, be part of growing consumer market and Indian legal framework's strengthening to accommodate these changes, generating Legal Capital for India's Seniors Citizens, who empowered can change perception from being vulnerable or probable victims to a valued assets.

INTRODUCTION

While addressing in 2017, 5th Global Cyberspace Conference, New Delhi, Honourable Prime Minister of India Mr Modi took serious commitment to formulate a strong cyber security framework and necessary regulations, all to promote the philosophy of 'Digital Indian Initiative', to have "a digital democracy" where all vulnerable and marginalised group can also have collaboration, inclusive participation to enjoy and improve living standards, technology eased living, sustainable development of society, economic resources with active use of Cyber and information communication technology and formulating supportive , stronger cyber security regulation policies, laws to address global issues of terrorism, radical State actions against developing societies. Where people's cyber-security awareness and alertness is developed to include init as a way of life. Cyber space must be utilised and exploited by all citizens 'inclusively' with equality of access and opportunity to have major contribution to world's usage of internet and social media for one's benefits. So, as to have State's sustainable development of cyber diplomacy, security, socio –legal growth thereby leading to empowerment and development of all.

The major cyber threats born by developing nations can hamper countries' growth in all aspects and comprehensive collaboration of all the stake holders, Industries, private sector, States and citizens along with international coordination can help promote a safer, securer cyberspace especially for migrants to information communication technology as stated in his speech 2020, New Delhi on Republic Day. Thus, providing the much-needed Government's will to bring in new change, laws, regulation policies in the field of Information and data sharing, exploration for the societal utmost benefit. The academicians 'and reformers in the lap of perfect timing to formulate comparative cyberspace framework most suited to Indian scenario, challenges faced by consumers of such cyber world, barriers such as cybercrimes perpetrated against the State to destabilise its growth, victimization faced by marginalised groups in developing societies and how stringent legal framework can address security concerns in cyber world.

A projected study done by World Economic Forum Global Risks (Report 2012) cites that by 2050 – World's urban population will double by 8.9 billion facing severe income disparities with fiscal imbalances with have direct effect on the development of new innovative ways of income generation and communications among societies. The General Assembly of United Nation (resolution 65/230) proposed to amend already enforced or new domestic and international legal frameworks to equip one to face challenges so germinating from complex exploitation of data and information technology by different consumers for fulfilling their needs and intentions. It further guided the States the states to indulge in various comprehensive studies on the challenges, problems prone to grow in cyberspace, the consequential cybercrimes and what could be innovative responses to cybercrime.

Universal Design of Inclusion for all strata especially **marginalised group,** who are facing an opportunity to increase their skillset of computer technology, including themselves in banking transactions, online education and working or using digital media in their lifestyle but, due to ramped increase in cyber crimes targeting Government, companies and vulnerable sections of society such as women, children and senior citizens is hampering this vision of inclusion. Knowledge with awareness of such cybercrimes plays the vital link for preventing such crimes, which is unevenly spread among these marginalised group due to their already weakened socio economic and political contribution, due to lack in legal capital to report and seek justice, they are re victimised and blamed due to social bias, not taken serious due to numerous disabling factors by the investigating authorities. But, as a progressive society legal frame work have addressed the issue of not having strong laws which need seriousness in investigation, reporting, maintain database and data for comparison and fast trials of such cybercrime case. ‘**Digital Literary’,** communication and networking’s aim are **active participation or inclusion** of all, irrespective to their age or needs in any given society.

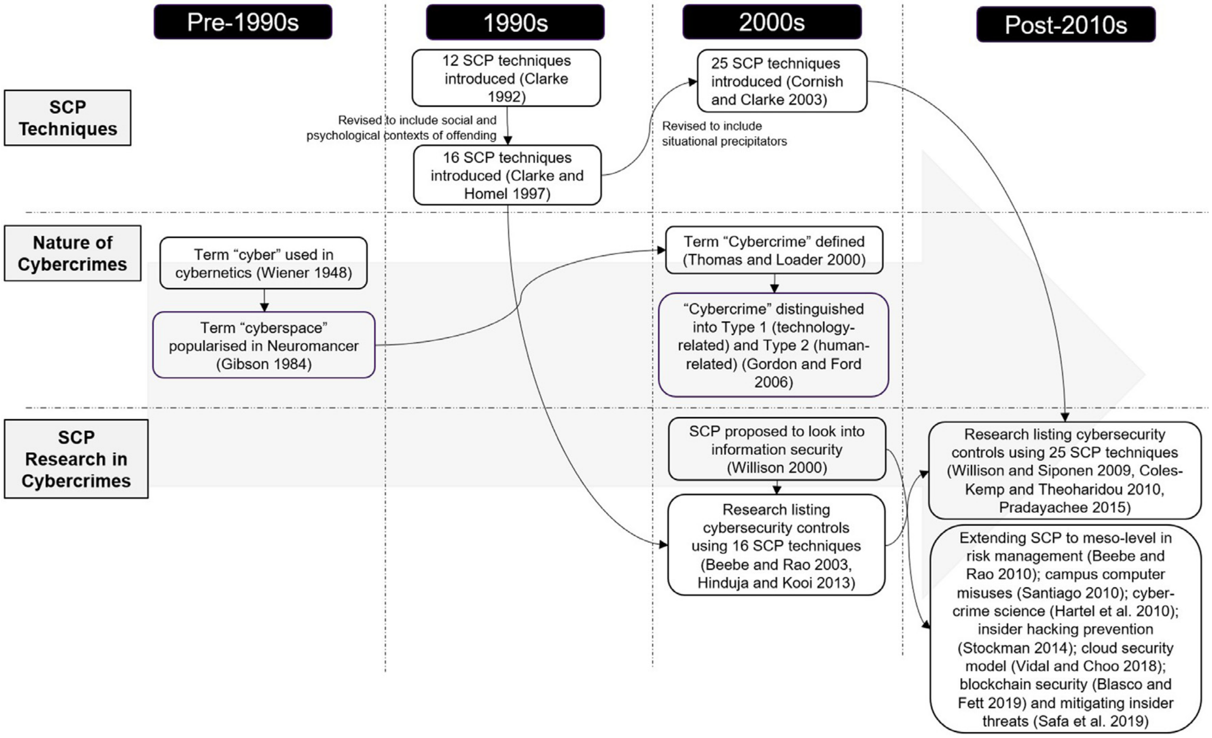
CYBERCRIME AS A PHENOMENON

Declaration of Salvador on Comprehensive Strategies for Global Challenges, 2012 in support to UN’s (resolution 65/230) observed that “*Development of Information, Communications Technology along with increased use of internet, will create a space for new possibilities for original criminals and new offenders to also switch from committing crimes in real world and virtual cyber world. Cybercrime will be a growing, contemporary challenge for States, which shall be driven by underlying socio-economic factors as unique to each Nation”.*

India’s marginalized sections are similarly hit apart from cyber attacks perpetrated against the Governmental establishment and corporate sectors. The groups were already facing exclusion from social, cultural, economic, legal and political unequal power distribution and relationships dimensions with other section shall be most vulnerable as seen with cybercrime cases perpetrate against women, children and senior citizens, who are made

> “ DEVELOPMENT OF INFORMATION, COMMUNICATIONS TECHNOLOGY ALONG WITH INCREASED USE OF INTERNET, WILL CREATE A SPACE FOR NEW POSSIBILITIES FOR ORIGINAL CRIMINALS AND NEW OFFENDERS TO ALSO SWITCH FROM COMMITTING CRIMES IN REAL WORLD AND VIRTUAL CYBER WORLD. CYBERCRIME WILL BE A GROWING, CONTEMPORARY CHALLENGE FOR STATES, WHICH SHALL BE DRIVEN BY UNDERLYING ~~SOCIO-EC~~ONOMIC FACTORS AS UNIQUE TO EACH NATION
>
> Declaration of Salvador

easy victims and are unable to make use of rich Legal Capital of Nation on cybercrimes. 'Cyber' term is taken from Greek word 'steersman' by Wiener in 1948, in fields of "cybernetics" meant as communications, control between machines and animals. Later Gibson in 1984 from this novel 'Neuromancer' created this term 'cyberspace'. Thereafter, word was widely applied to activities done within computers virtual space e.g. cybercrime, cybersex, cyber surfing etc.


Pre-1990s
1990s
2000s
Post-2010s
SCP Techniques
12 SCP techniques introduced (Clarke 1992)
Revised to include social and psychological contexts of offending
16 SCP techniques introduced (Clarke and Homel 1997)
Revised to include situational precipitators
25 SCP techniques introduced (Cornish and Clarke 2003)
Nature of Cybercrimes
Term "cyber" used in cybernetics (Wiener 1948)
Term "cyberspace" popularised in Neuromancer (Gibson 1984)
Term "Cybercrime" defined (Thomas and Loader 2000)
"Cybercrime" distinguished into Type 1 (technology-related) and Type 2 (human-related) (Gordon and Ford 2006)
SCP Research in Cybercrimes
SCP proposed to look into information security (Willison 2000)
Research listing cybersecurity controls using 16 SCP techniques (Beebe and Rao 2003, Hinduja and Kooi 2013)
Research listing cybersecurity controls using 25 SCP techniques (Willison and Siponen 2009, Coles-Kemp and Theoharidou 2010, Pradayachee 2015)
Extending SCP to meso-level in risk management (Beebe and Rao 2010); campus computer misuses (Santiago 2010); cyber-crime science (Hartel et al. 2010); insider hacking prevention (Stockman 2014); cloud security model (Vidal and Choo 2018); blockchain security (Blasco and Fett 2019) and mitigating insider threats (Safa et al. 2019)

Key genealogical developments of Situational Crime Prevention research in cybercrimes.

SCOPE

"*Cybercrime is a major challenge to a developing society and digital economy, Europol's priorities are to fight cybercrime threats*" – As per 2017's report by European Union Serious, Organised Crime Threat Assessment (SOCTA) body under Europol. At global level, Cybercrimes fall under 2 broad distributions either

i) Finance or

ii) Content motivated done to illegally manipulate accessibility, integrity and confidentiality of system and date depends on varying risk to both Governments, corporate sectors.

UNDOC have reported that copyright infringement will effect 24 % of the global traffic and 2/3 countries have cities their investigating agencies' statistics on cybercrime to be insufficient very important for policy making and comparison studies, recording of statistics is depended on development of that country, specialization of investigators, crime rates, underlying traditional crime rates with conviction to victims' compensation ratio and for online phishing, consumer frauds where data theft or breach is due to phishing or similar cybercrime techniques where cyber criminals use tools such as bot nets, malware viruses, social engineering techniques to commit cybercrimes. Content targeting women and children is pornography, grooming, cyber bullying. In case of senior citizens identify theft, online consumer frauds, phishing, romance scams are rampantly defrauding them directly raising legal and human rights concerns. Perception attached in mind of criminal is that they lack legal, computer knowledge, reporting or taking action skills and pool of surplus, saved funds make good targets with least investment. Victims' isolation and online victimisation causes serious health issues, lacunas in prosecution of cyber criminals, what can be the barriers to speedy justice *Victim Precipitation Theory* was seen functioning. Thus, making its scope a synthesis of multiple disciplines such as national security, criminology and justice system, legal and policing laws, medical health, banking guidelines etc. as applicable to medical science and forensic of a given crime scene, here related to cybercrimes.

NATURE OF CYBERCRIME

Cyberspace is a virtual space where cybercrime phenomena occur which is not mere interconnected computer systems or networks only, it involves direct opportunities and extent the computers, internet, informational technology present. Considering general criminological theories, it can be observed that cybercrime is *'a new, distinctive format of crime'* where both aspects of a criminal are projected onto a victim and the crime scene i) conforming that is legal and ii) nonconforming that is illegal behaviours when compared to real world. It is observed that cybercrime perpetrators may not commit physical crime in real world, reason being their status in society or psychological such as flexible timing, dissociative ego centric or anonymity attached with virtual identity, lack of real time deterrence or reaction when acts done otherwise. Cybercrimes are distinguished into 2 categories

i) Cyberspace Dependent e.g. Ransom ware attack

ii) Cyberspace Enabled e.g. cyber bullying

Financial with cyber dependent revolve around as hacking of Governmental, corporate's databases, senior citizens' personal information e.g. credit, banking credentials, capturing websites or networks. Whereas Content and cyber enabled are those traditional crimes which due to innovation and development of information technology have morphed by newer modus operandi to inflict heinous crimes against vulnerable children and women such as online frauds, cyber stalking, bullying, pornography and child sex tourism or trafficking for forced prostitution. Raising the inherent questions on which answers are yet to be sought such as, are we as society dealing with a novel type perpetrator generation with altogether different mens rea (motives), characteristics or it just same older generation of criminals who have upgraded themselves to now inflict their crime onto set of victims who are always perceived to be vulnerable, subjected to traditional abuse offline? Is it both? What can be comprehended as difference between cyber enabled criminal and cyber dependent?

More studies aimed at profiling is needed as it has been observed in some multidisciplinary researches that cybercrime perpetrator does have different motives, characteristics when compared to traditional offenders. *Social Learning Theory* in respect to *General Theory of crime*, when applied to cybercrimes states that the perpetrator needs to learn special, specific skills of internet, software, computer operating knowledge and seek out those persons who have or are perceived to have reduced self-control, likewise in virtual platform just as in real world. Time required to committed online crime is less, faster and have broad geographic outreach, perpetrator need not be in physically present e.g. sexual predator in cases of child molestation have to invest time, resources money to groom the victims whereas online predators will reach out in short time to huge number of potential victims via social media friendship, chatting etc. methods.

REASONS MARGINALISED ARE TARGETED

As per Cohen and Felson, **Routine Activity Theory** there is a unity of 3 factors a) Absence of Guardian, b) Suitable Target, c) Motivated Criminal , behaviour and intersection of people in time, space give rise to opportunities for a crime to be committed. Motivation cans both economic financial profit gain, ego driven and no motive at all just for fun or compulsion to do it. Can absent caregiver or family member be sought as an opportunity in cases to senior citizens, children and Women? Vulnerability is accompanied by age. But, having family, friends, caregivers act like a barrier for these marginalised group to avoid victimisation or helps in seeing the 'red flags' for avoiding falling in prey or prevention of fraud and cyber crimes aimed at them. Routine theory can be criticised as giving its focus on perpetrator, victim and methodology only, not on motive or causation, what is giving motivation to perpetrator or victim to get entangled in this vicious cycle of crime. Is it poverty, drug abuse, power need etc.? Who qualifies as the right target? Old age, illness, gullible or isolated or savings, available data, street children or young students, working women?

1. Cybercrimes which involved manipulation to commit frauds, cybercrimes, pornography, obscene content of children and women used as a product for marketing consumption of that strata of society which are addicts and sales schemes to defraud seniors etc. involves a sophistication, it is not like regular crime committed in streets, education and expertise of criminals cannot be ignored, formation of a fake company, hierarchy and group involvement cannot be undermined, committed very professionally as if running an organisation or company having formal hierarchy, taking each crime as a project, having hackers, data procuring subordinates, telesales team with convincing skills with managers and main boss, even though victims are sought as they are spending considerable time online, using applications, social platforms, shopping or studying online. The shared profile enables perpetrator to seek out those who will easily fall prey. Short term risk, less investment, huge profits Criminals are found to be younger usually not ethnic minorities, men having intellectual mind who are educated having higher socio-economic status when compared to traditional criminals.

2. Cybercrime are peculiar as has **international, transnational or interstate territorial, organised** involvements of different players, involves **grooming of the victims** into disclosing their personal financial details, getting abused or share their photographs and personal information, **social engineering techniques** are used to manipulate and isolate victims. Investigations are global effecting sovereignty, jurisdiction of states with extraterritorial evidence gathering and require international cooperation. A transnational dimension to a cybercrime offence arises where an element or substantial effect of the offence is in another territory or where part of the *modus operandi* of the offence is in another territory. International law provides for a number of bases of jurisdiction over such acts, including territory-based or nationality-based jurisdiction. Inconsistency of laws, regulations across country borders makes it especially difficult for countries to cooperate when investigating cross-border cyber-crimes, the opportunity of encountering cybercrime is developed with connectivity to world wide web for professional or social engagements.

3. To assert territorial or nationality jurisdiction, whole offence must take place in same country and it has been observed that sometime location of server, computer on which certain software are run, foreign service providers or perpetrator are differently located cross border, time is lapsed due to diplomatic or international agencies interactions which was in practise since *Lotus case of* Permanent Court of International Justice "the first and foremost restriction imposed by international law upon a State is

not to exercise its power, any form in territory of another State. But, the rules have evolved to secure balance (lex ferenda) and in matters of cyber stability and security as seen from Netherlands (*Bredolab* and *Descartes* cases) Dutch agency conducted cross border, non-consensual unilateral cyber operations against botnet, server holding child pornography content. Mr Dan Svantesson, have advised that States can adopt a middle path (4th in between category of jurisdiction) called "**investigative jurisdiction**" that may not be perceived as full attack on sovereignty or access to content subjected to cybercrime. Budapest Convention, **Article 32(b)** is an exception to general rule that prohibits trans-border access into stored computer data (not apply where location is uncertain). Tallinn Manual (International Law Applicable to Cyber Operations) also recommends remote viewing, downloading data at public platform to be taken as extraterritorial action as publishers already consented to its legal use, even though web-crawlers, data scraping tools will infringe the contractual terms

INDIAN'S EFFORT TO CURB CYBERCRIMES

"India is ranked 4th among the top 50 countries in terms of the number of cyber-crime complaints reported to the Internet Crime Complaint Centre" report by The Telegraph (2015)

Committed to align the domestic policies with the international **Convention on Cybercrime (2001**) held in Budapest, which is a multi-lateral, binding treaty, to promote cooperation and having a strong model for all UN Member States to promote harmonization of domestic cybercrime laws as per the international standards to address issues of sovereignty principles, extraterritorial data, investigation, law enforcement and prosecution assistance, prevention and combating cyber wars or terrorism. Indian's Legal framework maybe not perfect. But, it is very good, at par to Convention's standards and further amendments with make it secure and stronger.

A. **Legal framework - Information Technology Act**, **2000** on UNCITRAL Model of electronic Commerce have sections in regard to cybercrime(not spam or squatting yet), it is a strong digital law and with 2008 amendments' to sections 43, 66, 66(a) to 66(f) got itself aligned with Budapest Convention, where the basic question of Transnational nature, mutual cooperation among states, applying extraterritorial jurisdiction, gathering of evidence spread at global locations, investigation and procedural aspect of these cybercrimes was addressed. Still, not perfect and needs amendments and supportive laws to be arrive at an international common platform, so to take active cognizance of cyber security issues, maybe in future, it will be in Indian's benefit to give assent, rectify and commit to Budapest Convention, even though Government's current stand is to not surrender sovereignty and data sharing for security reasons In 2019 amendment to Act, make it mandatory that data of Indian citizens must be stored within territories of India.

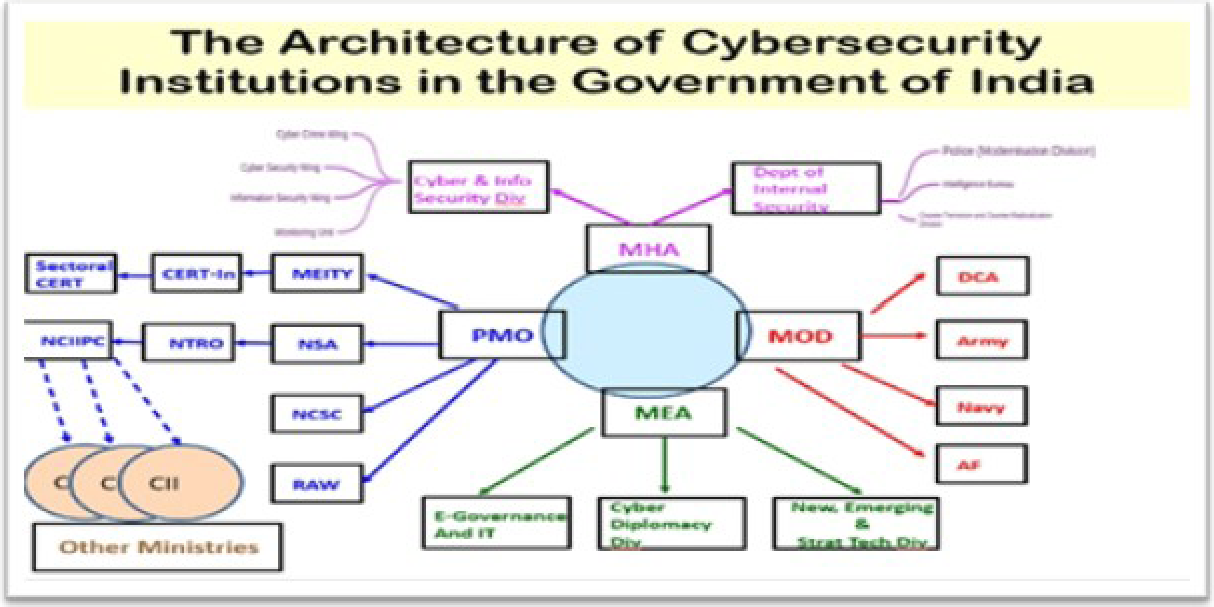
- **Constitution of India** - Guaranteed fundamental rights by Article 14, 19 and 21 ensuring citizens enjoy right to freedom equality, speech, life and dignity. Cyber-crimes infringed the privacy create a sense of insecurity and causes socio economic monetary loss to nation.

- **Indian Penal Code - The** Criminal Law (Amendment) Act, 2013 inserted 'stalking' a crime under **Section 354D**, online or offline are recognised, **292** (distribution of disgusting pictures), **354C** (Voyeurism against women),**499** (Defamation) , **354A** (offence of sexual harassment)

- **IT Act, 2000** - Section 84C (Attempt to commit crime), 66A (sending offensive messages), Section

66A of IT Act (sending hostile messages through correspondence), 67, 67A, and 67B (discusses punishment on erotica of children's),66E (punishes voyeurism against both genders), 66 C (identity theft), 66E (violation of right to privacy), 67 (Obscene Material in Electronic form)

B. **Government of India's initiative -** Has taken up following policy support to prevent cybercrimes, Data Security Council of India, Emergency Response Team (CERT), Terrorism Centre, USA – India's Cyber Security Forum, Information Security Assurance Programme, Anti-Bot Alliance, Tracking Networks for criminals and crime, intelligence grid, National Crime Records Bureau, National Cyber Coordination Centre.


The Architecture of Cybersecurity Institutions in the Government of India
Cyber Crime Wing
Cyber Security Wing
Information Security Wing
Monitoring Unit
Cyber & Info Security Div
Dept of Internal Security
Police (Modernisation Division)
Intelligence Bureau
MHA
Sectoral CERT
CERT-In
MEITY
NCIIPC
NTRO
NSA
PMO
MOD
DCA
Army
Navy
AF
NCSC
RAW
MEA
C
C
CII
Other Ministries
E-Governance And IT
Cyber Diplomacy Div
New, Emerging & Strat Tech Div

- National Cyber Security Policy, **<u>Indian Computer Emergency Response Team (CERT-In)</u>** <u>based</u> on **Section 70B of IT Act (**State of Ransom ware 2021 reports, **over 6,00,000 cyber security criminal offences are registered in India**.) takes care of Security breaches, frauds and data leaks are in direct proportionality, increasing with an increase in commercial online business activities of pan Indian's corporate entities.
- **<u>Data Security Council of India (DSCI)</u> -** Best practices and frameworks, publishes studies, surveys and papers aim to strengthen the security and privacy culture in the India.
- **<u>National Critical Information Infrastructure Protection Centre (NCIPC)</u>** - Cyber forensics activities, annual CISO Conference for Critical Sectors awareness and training.
- **<u>National Intelligence Grid (Nat grid) project of India</u> –** To counter terrorism measure that collects, collates a host of information from government databases including tax and bank account details, credit card transactions, visa and immigration records and itineraries of rail and air travel.
- **<u>Data Protection Bills, 2022</u> -** Which is upcoming new law (need law against spam or amendments to IPC or IT Act).
- **<u>The Information Security Practices and Procedures for Protected System Rules, 2018</u>** - As per **Section 70** of the IT Act. Government has passed to give access to only authorized person in a protected system/ server.
- **<u>National Nodal Agency / National Critical Information Infrastructure Protection Centre</u>**

under **Sec 70A** of the IT Act – Team deals with cyber security, operation technology, overall security of critical information infrastructure, policies which are resilient and robust to protect nation against cyber terrorism, cyber warfare etc.

- **Telecom Regulatory Authority of India (TRAI)** - limits SMS spam, unsolicited telemarketing sms, maintains 'Do Not Call list' and customers portal, imposing charges.

In 1970's Indian's 1st cyber-crime was committed by trunk calls/telephones and by 1980's proper cyber cases started to get registered in India by victims Few solved cases are as following - **PayPal Case** (Hacker put a loop to double money), Credit card stolen data used to book airline tickets, Love Bug spam mail to infect system and data, Online fake universities' degree frauds, **Kohli Online stalking of Delhi**, **Dubai blackmail and false identity**, **Chowdhury and Johnson (2008)**, **Matunga's Khalsa College Wifi hacking**, **Brain visa Technologies** Cases etc.

VULNERABLE GROUP EFFECTED BY CYBERCRIMES

National Crime Records Bureau reports cases for publication of sexually explicit content online is increasing by 110% from 6,308 to 3,076, with total of 306 cybercrime cases were registered against children in 2019 increasing to 1,102 cases in 2020.

Women and Children – face **cyber stalking** which is online harassment, expansion of cyber **bullying** leading to harassment, torture, physical threats, defaming to leak the private data or morphed photos of victims or information to harm the reputation of women, **Online Sextortion**, to circulate sensitive material on the internet in demand of seeking sexual favours resulting as online abuse, **Morphing** of photographs women, young girls, **Voyeurism** watching unsuspecting women or children in changing or toilets**, Online Child Grooming** to abuse them and **Digital** Rape inserting objects or human parts apart from penis in the vagina, ass or mouth of victim forcefully without consent.

Senior Citizens – faces Consumer phishing online frauds these kinds of cybercrimes which are illegal access to their personal secure data via computer networks, **online or tele caller frauds**, **identity theft** to procure financial gains, **fake charity** contributions, Life insurance/ savings, **romance** frauds and **vandalism**

CONCLUSION

The impact of trauma was seen in subconsciously distancing from being labelled as a victim, being weak, vulnerable All the studies aimed at seeking a solution at all levels to address the growing phenomena of Cybercrime victimsation of senior citizens, recommending formation or renewing a community support system on Cyber space, cyber security, crimes, types and procedures to follow if cybercrime is perpetrated specifically addressing concerns and needs of Senior adults. So that senior citizens can be included and migrated into advancing technologies and form a part of "Digital Society" be able to engage in all-inclusive digital. The states' s effort especially countries of Asia are amending their laws to get aligned with Convention of Budapest, making data protection policies, making it illegal to publish, use communication technology for obscene materials involving children, women in most Asian states even though erotica notion of nudity is culturally acceptable concept from country to country.

Therefore, any forthcoming Cyber security regulation policies must consider right to privacy, having either model of centralised or delegated model with a Main organization to lead the entire responsibilities of cyber security, taking all stakeholders interests collectively in a balanced way, planned or accessed risk with national incident, defensive and response plan supported by a data protection framework. Software Asset Management plan at par with international standards will help in managing redundant unlicensed software. A Research and Development team shall inform the government on advancement in this field and create rich partnership between private and public sector. Awareness with diversity initiatives at school curricula will educate on cyber breaches, hygiene, governments commitments and international policy. Cyber security policies approach should be i) Adaptable ii) encourage collaboration iii) internationally aligned iv) protect privacy. _

REFERENCES

1. Simasathiansophon, N, Chaisongkram, P, Kaewsaiha P, Boonarchatong K. (2021) "Enhancing Digital Literacy of Senior Citizens", Eurasean: journal on global socio-economic dynamics", Volume 5 (30)
2. Relia Sanjeev (2021) "Cyber Security Risk Mitigation Road Map for CISO and CIO as Business Drivers", Analytics Insight digital magazine
3. Department of Justice, Office of Public Affairs, Justice news, Tuesday, June 11, 2019
4. Mazerolle Lorraine, Ryan Koa, Heemeng Hoa (2022), "Situational Crime Prevention (SCP) techniques to prevent and control cybercrimes: A focused systematic review"
5. Independence day speech of PM Modi,"India will soon introduce a new cyber security policy" published in Indian Express, August 15, 2020
6. Gautam, R., Kulshrestha, P., & Goswami, M. A. K. (2021). Mediation And Family Dispute Resolution Mechanism: A Case Study On Clinical Legal Education. Elementary Education Online, 20(3), 2490-2490.
7. Gautam, R., "Proliferation of Cyber Crime and Indian legal system with special reference to Gwalior Division" Available at: https://shodhganga.inflibnet.ac.in/handle/10603/250817 Retrieved on: 22/07/2021
8. Pandey, N., Gautam, R., "property right of women in patriarchal indian society: a comprehensive study on legal narrative" Available at: https://www.researchgate.net/publication/361733554_property_right_of_women_in_patriarchal_indian_society_a_comprehensive_study_on_legal_narrative_property_right_of_women_in_patriarchal_indian_society_a_comprehensive_study_on_legal_narrative
9. Gautam, R., Medical health condition of prisoners and discrepancy in facilities among the states of Uttar Pradesh, Haryana and Delhi, International Journal of Health Sciences Follow journal, DOI: 10.53730/ijhs.v6nS6.12256
10. Gautam, R., Kanpur Philosophers ISSN 2348-8301 Vol IX, Issue v (iv), 2022151efficacy of proceedings of conciliation and settlement of anindustrial dispute under industrial disputes act, 1947, a critical Analysis. Available from: https://www.researchgate.net/publication/361733673_Kanpur_Philosophers_ISSN [accessed Sep 11 2022].
11. Schiks Jim, Steve G.A, Weijer van de, Leukfeldt Rutger (2022), "High tech crime, high intellectual crime? Comparing the intellectual capabilities of cybercriminals, traditional criminals and non-criminals"
12. Deka Chayanika (2018), "Global Conference on Cyber Space"
13. Archick, K. (2006), 'Cybercrime: The Council of Europe Convention', Washington, DC: The Library of Congress
14. Pande Jeetendra (2017), "Introduction to Cyber Security", Uttarakhand Open University, ISBN: 978-93-84813-96-3

2

CYBERCRIME AGAINST WOMEN, CHILDREN AND SENIOR CITIZEN

KEYWORDS

CYBERCRIME, WOMEN, CHILDREN, VICTIM, OFFENCE, CRIME AGAINST WOMEN

CHAPTER TWO

CYBERCRIME AGAINST WOMEN, CHILDREN AND SENIOR CITIZEN

AUTHORS

AISHWARYA RAJPUT, LL.M (CORPORATE AND COMMERCIAL LAW), SHARDA UNIVERSITY, GREATER NOIDA, INDIA

PROF. PRADEEP KULSHRESTHA, DEAN, SCHOOL OF LAW, SHARDA UNIVERSITY, INDIA

ABSTRACT

In present day scenario, the cybercrime is on the verge of rising and everyone is being a victim of such cybercrime which are happening worldwide by just a click on the computer and with the internet. The advance technology of the internet has definitely threatened the legality of the laws. Any person having an access to the internet and knowing how to operate a computer can easily commit the offence of cybercrime. Everyone has been a victim of cybercrime in their life sometime or the other. The existing norms and clauses of the criminal law seems to be ill equipped and outdated to deal with such advance crime happening in the cyberworld. Women and children have always been a target of any crime and likewise, the cybercrime against women has also taken the lead. Women are now also being subjected to the cybercrime and there have been many instances where we can see the females and the children being the easy target, even in the cyberworld.

In this paper I shall plan to discuss how the cyberworld has affected the women, children and senior citizen of the country. I shall also briefly examine upon various

existing laws that deals with specific aspects of the cybercrime and also crime against women and children. I will be referring to various case laws to interpret the objectivity of the cybercrime and also refer the major sections of The Information Technology Act (2000) and The Indian Penal Code (1860). In this paper, I shall further describe what exactly a cybercrime is and what the various types of cyber-crimes are. I will be elaborating the reasons of such offences and how an individual is being a victim under cybercrime, especially women, children and senior citizen. At our conclusion, we will focus on methods and judicial remedies available to prevent such cybercrimes.

INTRODUCTION

Cybercrime in general may be defined as 'Any unlawful act where computer is used to commit or facilitate the crime. It includes all the criminal activities carried out by means of computer, and the internet.

The term 'Cybercrime' has been defined under Section 65 of The Information Technology Act (2000).
It is as follows:

Section 65 of The IT Act (2000) says a person who intentionally conceals or destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer program, computer system or network when the computer source is to be required to be maintained by law is punishable with imprisonment upto 3 years or with fine that may extend upto 2 lakh rupees or with both.

'Computer source code' means the listing of the programs, computer commands, designs and layout and program analysis or computer resource in any form.

Crime is basically a social phenomenon and is as old as the civilization. With the growing advancement and rapid technology, most people have been a victim of cybercrime and other penal crime but women and children have always been an easy target due to the societal difference and growing concept of the men v/s women. The concept of cybercrime is not much different from that of the concept of conventional crime. Both include the breach of rules of law and counterbalance by the state.

CYBERCRIME AGAINST WOMEN

Nowadays, crime against women and children is rising very rapidly and likewise, cybercrime against women and children is on the verge of rising. Most of the people are facing cybercrime but almost every second, a woman is being a victim of such crime, reason being the disparity and the societal difference that some people have created for the women and also due to lack of proper knowledge.

The constitution of India guarantees equal rights to life, education, health, food and work to women but the same modesty of a woman seems to be diminished and no specific provisions have been made to protect the privacy or modesty of a women or children when facing any such cybercrime.

There are no specific provisions in the Information Technology Act (2000) for the cybercrimes committed against women and children. Cybercrime has thus become a hard reality in India, difficult to detect and also quite difficult to prevent. Paperless contracts, digital signatures, online transactions and cyber crime have taken the legal world by surprise. Most of the time, the perpetrators get a chance to harass, abuse or blackmail the women and children more because they tend to lack proper knowledge of dealing with cybercrime. The cybercrime against women is mostly done by creating fake accounts on social networking site such as Facebook, Twitter or Instagram. Women are also being trolled and objectified on many basis over the social media. The accused tend to post bad comments over the pictures of women and try to harass them by some sort of blackmailing, threatening or bullying.

It is hard reality of our nation that women are treated as objects and most men tend to suppress themselves over women because they think that it's some sort of a ritual or a rule that women need to be submissive to any male in their life and the male is always supposed is the main reasons which leads to cybercrime against women and children.

MAJOR FORMS OF CYBERCRIME AGAINST WOMEN

Due to the commission of cybercrime, many women go through a lot of rough time in their lives and undergo hypertension, depression, anxiety and other adverse health issues. Women and children are the easiest target for perpetrators to commit crime against, be it conventional crime or the cybercrime.

Following is some of the most common cybercrimes that are committed against women and children worldwide. They are enumerated as below.

1. **Cyber Stalking**: This is a form of cybercrime which involves two persons, firstly the stalker, also called the attacker and secondly the women (victim) who is harassed by the stalker. Women nowadays have been the target of cyberstalking. It is basically a way to stalk or peep into someone's social media profile continuously, in an inappropriate way which directs to online harassment and online abuse. The cyberstalking involves using the internet, cell phone and any other electronic device used to stalk another person. Section 354D of The Indian Penal Code (1860) defines the term Cyberstalking.
2. **Harassment through email**: Harassment through email has become a very common type of cybercrime which is being conducted against women and children on a large scale. It includes bullying, threatening, cheating and blackmailing via email.
3. **Phishing**: Phishing is a type of social engineering where an attacker sends a false message created to manipulate the person with the intention to fraud them.
4. **Cybersquatting**: It is the practice of registering names, especially well-known companies or brand names, as internet domains, in the hope of reselling them at a profit.
5. **Defamation**: Cyber defamation includes libel as well as defamation. The offence of defamation is punishable under Section 500 of The Indian Penal Code with an imprisonment of upto 2 years or fine or both. The law of defamation under Section 499 got extended to "Speech" and "Documents" in electronic form with the enactment of the IT Act, 2000. The publication of material which intends to harm the reputation of the individual or organization, and such publication done via a computer and with the help of an internet, tends to constitute the offence of cyber defamation under the cyberworld.
6. **Morphing**: Morphing is simple editing the image of a person with a fake identity by an unauthorized person (the attacker) which is intended for some wrong purpose. The pictures of the females

are downloaded by fake users and re-posted on the social media by creating fake profiles. The cybercriminals misuse the pictures of women by editing them with the morphing tools available on the internet and somehow promotes pornographic content.

7. **Trolling**: This is one of the most common cybercrime that is being committed against women and children in the cyberworld. Trolls spread conflicts and quarrels on the internet and the attacker posts bad or defamatory comments in an online community against the women which upsets them and causes severe anxiety, depression and other major health problems.
8. **Child Pornography**: Cyber pornography is another threat to the female netizens. There are various provisions under The Information Technology Act (2000) and The Indian Penal Code (1860) which regulates and prohibits child pornography. Section 67-B of the IT Act, 2000 makes publishing, transmitting, viewing or downloading child pornography illegal. Any person who has not attained the age of 18 years is a child. Section 292 of The Indian Penal Code prohibits the sale of obscene material. Also, the Protection of Children from Sexual Offences Act (2012) was enacted to protect children from the sexual offences. The act protects the children from sexual harassment, sexual assault and pornography. The act aims to protect the well being and interests of the children. The child pornography includes sexual content which intends to harm the modesty of a woman.

CASE LAW

The Ritu Kohli Case

The Ritu Kohli case is the first case in India which was dealing with cyberstalking. The Delhi police arrested the culprit, Manish Kathuria. In the said case, Manish was stalking a person called Ritu Kohli by illegally chatting on a certain website. Manish was chatting under the identity of Ritu Kohli and using obscene and obnoxious language. He was disturbing her residence telephone number and inviting to chat with her on telephone. Consequently, Ritu was getting obscene calls from other people, various parts of India and Abroad. Ritu Kohli reported the matter to the police and the Delhi Police swung into the action. The police had registered the case under Section 509 of The Indian Penal Code for outraging the modesty of a woman (Ritu). But Section 509 of the I.P.C only refers to words, gestures or act intended to insult the modesty of a woman. But when the same things are done on the internet, there are no such provision or mention about the same in the said section. Ritu Kohli's case was an alarm to the government to make laws regarding the aforesaid crime and regarding protection of victims under the same.

As a result, Section 66A of the Information Technology Act, 2008 states, "Punishment for sending offensive messages through communication service, etc:

Any person who sends, by means of a computer resource or a communication device, -

1. any information that is grossly offensive or has menacing character; or
2. any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will, persistently makes by making use of such computer resource or a communication device,
3. any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages shall be punishable with imprisonment for a term which may extend to three years and with fine.

CYBERCRIME AGAINST SENIOR CITIZEN

Like women and children, even senior citizens are also being targeted as a victim of cybercrime. Usually, the reason being that they lack the exact knowledge about the technology. They are not much aware about how to go along with the advanced technology of the internet and computers and hence, they too become the easy targets of cybercrime. Here are some forms of cybercrime that are committed against the senior citizens:

1. **Government impersonation scam**: The attackers or the criminals impersonate themselves as government employees and asks for money by threatening or blackmailing the old citizens. Unaware about such crimes, the senior citizens tend to fall into their trap of cybercrime.
2. **Financial scam**: Criminals target potential victims using illegitimate credentials from legitimate services.
3. **Cyberextortion**: Under this crime, the attacker or the criminal asks or extorts for money from the senior citizens by blackmailing them on the basis of certain grounds.

PREVENTION OF CYBERCRIME

The cybercrime against women, children and senior citizen is on the verge of rising and they are being attacked by the attackers across the globe. The Ministry of Home Affairs has initiated a scheme for the prevention of cybercrime against women and children and a mechanism to deal with the same.

Following are the components of the CCPWC scheme:

- Online cybercrime reporting unit
- Forensic unit
- Capacity building unit
- Research and development unit
- Awareness creation unit

PREVENTIVE MEASURES PROVIDED BY THE GOVERNMENT

1. **LEGISLATIVE SUGGESTIONS**: Special provisions need to be passed by the legislature which shall specifically deal with the cybercrime against women and children.
2. **JUDICIAL SUGGESTIONS**: A special bench of judges should be appointed in each High Court which shall specifically deal with the cases related to cybercrime against women, children and senior citizens.

SUGGESTIONS TO PREVENT CYBERCRIME

1. Always use strong passwords and do not share the passwords or username with any person
2. Proper knowledge regarding the use of the internet and computer should be imparted to everyone, especially the women and the children
3. Specific laws should be made by the legislature and shall be implemented in the nation
4. Avoid meeting any online friend alone as they are a complete stranger. Always prefer taking some trustworthy person along if ever meeting an online friend face to face
5. Block the person if he/she talks in an inappropriate way which targets the modesty or any other aspect which can be harmed

6. Limit the amount of personal information that you post on your social media
7. Avoid adding unknown people to your social networking sites such as Facebook, Instagram, Twitter or Whatsapp
8. Never send money or any personal bank details to any unverified person on the internet
9. Never share financial account or bank account details and do not allow anyone to access your accounts
10. Never open any attachment links from an unknown or unauthorized email address.

CONCLUSION

To sum up, we can say that cybercrime is a very ongoing type of a crime which is happening worldwide. The digital platform and social media are the main tools that are used to commit cybercrime. One needs to be very cautious and careful when using social media and accessing the internet. Women, children and the senior citizens need to be even more careful while using the social media because they are the ones who are largely targeted by the attackers. One should avoid sharing personal details on the social networking sites. Women need to be more courageous in reporting any type of unusual activity that they notice online. Although we have certain provision of the Information Technology Act and The Indian Penal Code which somewhat deals with the offence of cybercrime but there needs to be proper and specific provisions which clearly mentions and describes the cybercrime against women, children and the senior citizens.

REFERENCES

1. Gautam, R., Kulshrestha, P., & Goswami, M. A. K. (2021). Mediation And Family Dispute Resolution Mechanism: A Case Study On Clinical Legal Education. Elementary Education Online, 20(3), 2490-2490.
2. Gautam, R., "Proliferation of Cyber Crime and Indian legal system with special reference to Gwalior Division" Available at: https://shodhganga.inflibnet.ac.in/handle/10603/250817 Retrieved on: 22/07/2021
3. Pandey, N., Gautam, R., "property right of women in patriarchal indian society: a comprehensive study on legal narrative" Available at: https://www.researchgate.net/publication/361733554_PROPERTY_RIGHT_OF_WOMEN_IN_PATRIARCHAL_INDIAN_SOCIETY_A_COMPREHENSIVE_STUDY_ON_LEGAL_NARRATIVE_PROPERTY_RIGHT_OF_WOMEN_IN_PATRIARCHAL_INDIAN_SOCIETY_A_COMPREHENSIVE_STUDY_ON_LEGAL_NARRATIVE
4. Gautam, R., Medical health condition of prisoners and discrepancy in facilities among the states of Uttar Pradesh, Haryana and Delhi, International Journal of Health Sciences Follow journal, DOI: 10.53730/ijhs.v6nS6.12256
5. Gautam, Ritu, Cybercrimes and International legal regime, Available at: https://shodhganga.inflibnet.ac.in/bitstream/10603/250817/10/10_chapter-iv%20%20cybercrime%20issues%20and%20international%20legal%20regime.pdf
6. Gautam, Ritu, Cyber crime in India, Available at: http://hdl.handle.net/10603/250817
7. Gautam, R., Kanpur Philosophers ISSN 2348-8301 Vol IX, Issue V (IV), 2022151EFFICACY OF PROCEEDINGS OF CONCILIATION AND SETTLEMENT OF ANINDUSTRIAL DISPUTE UNDER INDUSTRIAL DISPUTES ACT, 1947, A CRITICAL Analysis. Available from: https://

www.researchgate.net/publication/361733673_Kanpur_Philosophers_ISSN [accessed Sep 11 2022].

8. The Information Technology Act, (2000) Section 65
9. The Information Technology Act, (2000) Section 66
10. The Information Technology Act (2000) Section 66-A
11. The Information Technology Act (2000) Section 67-B
12. The Indian Penal Code (1860) Section 292
13. The Indian Penal Code (1860) Section 354-D
14. The Indian Penal Code (1860) Section 500
15. The Indian Penal Code (1860) Section 509
16. The Protection of Children from Sexual Offences Act, 2012
17. The Ritu Kohli Case

3

CYBER CRIME: CHILD AS A PERPETRATOR, CHILD AS A VICTIM

KEYWORDS

PSYCHOLOGICAL FACTORS, CYBER FRAUD, CHILD PORNOGRAPHY, PROTECTION MECHANISM, CYBER SENSITIZATION

CHAPTER THREE

CYBER CRIME: CHILD AS A PERPETRATOR, CHILD AS A VICTIM

AUTHOR

AMAR KUMAR ROY, LL.M STUDENT, CHANAKYA NATIONAL LAW UNIVERSITY, PATNA

ABSTRACT

The web of cyber world is moving rapidly like a galloping horse with the introduction of novel technologies every second, penetrating its roots amongst masses and particularly in teenagers. At times, this penetration takes us to the dark side of this cyber web which entraps people into a pool of cyber-crimes, often affected by socio-economic as well as psychological factors. One of the most affected classes belongs to the group of children who often tend to fall on both sides of the curtain- at one side remains a child in the face of a perpetrator, on the other side is a child who becomes the victim. Both facets can be seen within offences like cheating by personation (often referred as cyber fraud), violation of privacy, publication or transmission of obscene materials, child pornography, cyber stalking, cyber bullying in educational institutions, etc. punishable under various legislations. Complexity in this field arises because of the fragile age of the perpetrator and need for diverse protection mechanism for victims. This has increased our burden, as apart from legislations and judicial decisions, there has to be sufficient mechanism for prevention and increasing awareness at a very early age so as to sensitize them of severity of these offences.

INTRODUCTION

The definition of Child is diversified in the eyes of law which very much depends upon the policy and purpose of the law. However, certain principles have always been adhered to while framing laws in relation to child, which has been provided in multitude of International Conventions and Frameworks and which has been further incorporated in legislations passed by Parliament.

The first and the foremost is the Universal Declaration of Human Rights which specifically declares that every child is entitled to special care and protection.[1] International Covenant on Civil and Political Rights[2] and International Covenant on Economic, Social and Cultural Rights[3] further strengthens the above declaration by putting an additional duty upon member States to provide measures for protection of children which are necessary due to his status as a minor and to provide for special measures for their protection from any economic or social exploitation respectively. Even though there was a range of protection and rights entrusted upon the child there was still a need to provide a uniform definition of the child. Recognizing the same, United Nations adopted Convention on the Rights of the Child which now defines child as every human being below the age of eighteen years.[4] India being the signatory has adopted the same definition for the purpose of identifying child under the criminal justice system.[5] This definition is universal for the purpose of identifying offenders as well as victims.

The matter related to child has always remain sensitive as it is an undeniable fact that they need special care and protection. This is why it becomes important to identify and scrutinize the various aspects when a child interacts with the cyber space. Cyber Space has no boundaries or limitations and can easily circumvent the set rules meant to regulate the same. This is why issues pertaining to Cyber Space in itself is considered opaque and hydra-headed. It interacts with every human being irrespective of age in this new world. The moment child is born and becomes capable of establishing some sort of communication in their surroundings, he is introduced of cyber technology in one form or the other. Practically, it is inevitable and in fact has more good than evil. Hence, there is an everlasting need to balance the good and evils of cyberspace to maintain an equilibrium in the society. However, there may arise problems when this balance will not be maintained. Moreover, problems related to a child is in itself problematic as understanding child psychology in a given set of circumstances is a complex task. Therefore, when a child interacts with the cyberspace, it aggravates. For that reason, there is a need to conduct proper study on the co-relation between child and cyberspace.

The researcher has tried to understand this inter-relation in the forthcoming Chapters and how law regulates this relation. The researcher in order to explain the same has referred to doctrinal mode of research and has relied upon existing studies on this issue and has also tried to put forth certain suggestions.

[1] Universal Declaration of Human Rights art. 25(2).

[2] International Covenant on Civil and Political Rights art. 24(1), Dec. 16, 1966.

[3] International Covenant on Economic, Social and Cultural Rights art. 10(3), Dec. 16, 1966.

[4] Convention on the Rights of the Child art. 1, Nov. 20, 1989.

[5] The Juvenile Justice (Care and Protection of Children) Act, § 2(1)(12)-2(1)(13) (2015); The Information Technology Act, Explanation to § 67B (2000).

INTER-RELATION BETWEEN CHILD AND CYBERSPACE

Today there has been a sea change in the psyche of the offenders who have shifted their mode of committing offences from traditional means to the internet due to the complexities involved in the enforcement of laws and collection of evidences in offences relating to cyberspace. It provides the offender a sense of security and they also consider this mode as safer and more efficient as now offences can be committed on merely a few keystrokes and ironically, internet also provides them a sense of privacy. Because of these characteristics only, it also attracts the juvenile delinquents who often tends to fall for these attractive overtures. On the other hand, the above explained reason also becomes a prominent reason to commit offences against the children.

In a significant study, it has been found that there are multiple evidences which shows negative clinical and neurological effects of the screen in front of us on the kids and the clinical research also suggests that a child may be introduced with various psychiatric disorders like anxiety, depression, increased aggression, etc. due to its prolonged use. These are the undeniable negative effect of the technology on the child.[6] And these signs are often ignored by the parents and this ignorance has been traced to the very root cause of offence of cyber bullying.

In another study conducted by Dr. Richard Freed, a renowned child psychologist, it has been further analyzed that only because a child is technology friendly or in another word, an expert in the technology, a parent shall not consider their child to be able to review or understand on its own the effects of technology on their lives. This is why there is a self-imposed duty upon the parents to guide their child in this cyber space so that the technology can be fruitfully enjoyed by their child.[7]

There is an abundance of information on the internet and it includes misinformation as well as ill-information and all are flowing indiscriminately. Therefore, not the information but clarity of the information is the power. So, it is very essential that a child must be well informed so that he or she may be able to judge or differentiate ill-information from the information. Naturally, a child cannot make a better judgment regarding the same. Therefore, there is an implied duty cast upon us, individuals as well as the legislators, to segregate the same in order to provide a better virtual experience to the child.

CHILD AS A PERPETRATOR AND CHILD AS A VICTIM

Child as a perpetrator

Edwin Sutherland, who propounded the Differential Association Theory, suggested that any person indulges in any criminal act only after learning the same in close social group. He further explained that one is not criminal from birth or does not inculcate the traits of a criminality on its own, rather, it is the result of one's interaction with its surroundings. This process of moving towards delinquency is same as learning any other skills.[8] The

[6] Nicholas Kardaras, Glow Kids How Screen Addiction Is Hijacking Our Kids— And How To Break The Trance, Chapter-1 Introduction, (2016).

[7] Richard Freed, Wired Child: Reclaiming Childhood in a Digital Age, (2015).

[8] Anthony Walsh & Craig Hemmens, Introduction to Criminology 144 (2d. ed. 2011).

same can be understood in the position of a child who is introduced of technology at a very young age and as discussed above internet carries with itself every kind of information. It becomes a big problem particularly in cyberspace as it is a complex environment wherein on a single platform everything is available, from educative content to incriminated content. Inability to differentiate among the two is the most challenging task for a child and it is for the legislators and other members of society to provide solutions for this menace. This is how internet works as a criminogenic element and motivates a child to commit a crime.

Another theory which would help us to understand as to why juveniles tend to become delinquent is the Social Disorganization Theory which has been propounded by Shaw and McKay. According to them, involvement of juveniles in crime is often due to factors including urban density, substandard housing, low income, inadequate schools and family problems. These factors result into social disorganization and often cannot be controlled by an individual.[9] This can be very well understood as just like our society there is also a digital divide of have and have-not(s). Although it may not be a prominent factor behind commission of cyber-crimes by a child but it may act as a force which pulls them towards committing the same.

On the one hand, it is said that the age of adolescence is the age of story and thunder as many ideologies, problems, thoughts and various ways of expression evolve in their mind at this age and on the other hand, it is a well-known fact that technology is a queer thing, i.e., it gives gift in one hand and stabs you in the back. It acts as a vehicle which provide its pillions plethora of things to get invested into. Therefore, when both of them meets in an unchecked environment, then, there may arise a situation of conflict between the child and the law and a juvenile is born.

A child in the cyberspace can act by himself without any interference by the other, they are freer than ever. This is so because of the transformative nature of the cyberspace, few of them can be listed as:[10]

a) Globalization: Cyberspace has expanded the limits of our culture as well as expanded the jurisdiction for those who wants to commit offences on this sphere.
b) Distributed Networks: Individuals are shaping their relationship with each other which involves flow of data among themselves and thereby also create avenues for victimization of an individual.
c) Data Trails: This transformative aspect has two approaches; one is that it acts as a tool for law enforcement agencies in their investigation and the other is that it creates a scope for identity theft.
d) Transnational Environment: It provides a whole new range of options to choose from in order to commit a cybercrime. Such options may include, dealing in sexually explicit materials, child pornography, cyber frauds, etc.

The above discussed factors may be one of the many reasons as to why a child gets attracted towards committing cyber offences and become a cyber delinquent and their victim can be anyone – an adult or a child or the juvenile himself.

Child as a Victim

[9] Richard Lawrence & Craig Hemmens, Juvenile Justice, 11 (2008).

[10] David S. Wall, The Internet as a Conduit for Criminal Activity, Book- Information Technology and the Criminal Justice System, (April Pattavina et al. eds., 2005).

Hon'ble Justice Krishna Iyer once said that the victim is the most neglected individual in our criminal justice system, he even coined the same as "vanishing point of our criminal law".[11] The observation made in 1979 stands true till date due to lack of proper redressal mechanism in our criminal justice system which is further encompassed with inordinate delays.

When we deal with child victims and that too in the cases relating to cyber offences, a special need and care has to be imparted upon them as even when the victim has not suffered physical trauma but mental trauma in itself is sufficient to torment the psychological state of such child. An additional duty is also cast upon the investigators and prosecutors as in majority of cyber offences, a child victim does not know have the knowledge of physical identity of the perpetrator which complicates the trial.

Cyberspace advancements has made many children as victims-in-waiting. From the outside, cyberspace may seem like safe, lawful and certain, but in reality, this advancement needs to be regulated for the sake of maintaining that seemed to be safe, lawful and certain environment. Otherwise, the whole process of victimization of child would affect the very course of one's life as victimization with itself brings a bundle of emotions that includes depression, anger low self-esteem and low self-efficacy.[12]

COUNTER-MEASURES

In order to regulate this cyber behavior among and against child, Parliament has enacted certain legislations creating certain offences punishable under the law and also protection for juvenile delinquents.

The Information Technology Act, 2000

Due to the rapid pace of technological advancements, there arose a need to enact a separate legislation due to which Parliament enacted this Act and thereby created a cluster of offences which were being committed in the cyberspace. While doing so, criminal liability was also introduced for commission of offences against child, which can be summarized as:

i) Violation of Privacy: The cases of violation of privacy is the most challenging for law enforcement agencies as it is in most rampant use by the offenders. It can be very well seen from the reports published in our newspapers which involves capturing of images of private parts of a female or child in changing rooms of the Malls or Clothing Stores, filming of one's person in public toilets, making the act of sexual harassment or rape go viral on various online platforms, extortion after threatening to circulate one's unpleasant photographs, etc. All of these cases has been made punishable under the Information Technology Act, 2000[13] in addition to the Indian Penal Code, 1860[14] and the Protection of Children from Sexual Offences Act, 2012.[15]

[11] Ratan Singh v. State of Punjab, (1979) 4 SCC 719.

[12] Anthony Walsh, Criminology, 261 (2012).

[13] The Information Technology Act, § 66E (2000).

[14] The Indian Penal Code, § 354C, 509 (1860).

[15] The Protection of Children from Sexual Offences Act, § 11 (2012).

ii) Publishing or transmitting obscene material: Here, the word "obscenity" has wider connotation than the word "pornography", the test of which has been laid down in the case of *Ranjit D. Udeshi v. State of Maharashtra*,[16] Supreme Court has held in this case that unless any act corrupts or deprave the mind to immoral influence, any act cannot be said to be obscene. Publishing and transmitting of such materials which may also include a child victim has been made punishable under Section 67 of the Act. However, this section was not sufficient to deal specifically with cases relating to child and hence 2008 Amendment inserted Section 67B in the Act, segregating the child pornography from the rest.

iii) Child Pornography: Even when children are considered to be a form of God in our country, the cyber revolution has increased the exploitation of child manifold. The main reason behind the same can be understood from the characteristics of the internet which provide anonymity to the offender with little or no expense on its own part. This is one of the various modes of committing child abuse. Firstly, pornographic videos or images are produced and then, further distributed and streamed on the internet and at times, pictures of children are also morphed to create such content.[17] To make such acts punishable, Section 67B was introduced which exhaustively punishes every act related to child pornography and includes within its sphere publishing, transmitting, creating, collecting, downloading, seeking, exchanging, distributing or recording a child in obscene or indecent or sexually explicit manner. This provision does not leave any gap or loopholes for the offenders to go around and commit this heinous offence.

There are also certain Cyber Offences punishable under the Information Technology Act, 2000 which has attracted children to become Juveniles who are later tried as per the Juvenile Justice (Care and Protection of Children) Act, 2015:

i) Dishonestly receiving stolen computer resource: Under this offence dishonest receiving or retention or having reasonable apprehension to have in one's possession stolen computer resource or communication device has been made punishable.[18] Here, 'communication device' may include smart wearable devices, mobile phones, laptop, tablet, etc. The above act has also been made punishable under Section 411 of the Indian Penal Code, 1860.

Many organized criminal group recruits' children as a member of their group and at times, children by themselves indulge in commission of the above-mentioned offence as they are aware of the fact that even if they will get caught, they will get diminished punishment under the criminal justice system due to the protection accorded to the children under the law.

ii) Cheating by Personation: Section 66D of the Act specifically incriminates cheating by personation committed by any person by any communication device or communication resource. The relevant instances in which a child commits this offence can be seen in cases of committing fraud by way of sending deceptive messages or emails on behalf of banking institutions, sending messages by requesting monetary help pretending to be a close family member or a friend, getting OTP through

[16] AIR 1965 SC 881.

[17] Talat Fatima, Cyber Crimes, 129 (2d ed. 2016).

[18] The Information of Technology Act, § 66B (2000).

voice phishing for an online banking transaction by deceiving the victim on some pretext or the other, running fraudulent schemes in the name of some reputed institutions, etc.[19] These are some of the methods employed by a juvenile cyber offender to indulge in fraudulent and illegal financial transactions.

OTHER CYBER OFFENCES CONCERNING CHILDREN NOT COVERED UNDER THE IT ACT

i) Cyber Stalking: Nowadays, in addition to following anyone in person has extended to the cyberspace as well and this has also been categorized as an offence and made punishable under the Indian Penal Code, 1860.[20] Section 354 D(2) of the Code specifically penalizes the act of any man who monitors use of any form of electronic communication done by a woman. When we would analyze the above provision, we can easily conclude that the above offence has been made punishable only when an act is committed by a man against a female victim.[21] This does not cover the situations wherein a victim can be a male child and offender a female and Parliament needs to fill this lacuna to prevent any such offence being committed against a male child. However, Parliament has enacted a special law to fill the above gap by classifying the above act as Sexual Harassment under Section 11(iv) of the Protection of Children from Sexual Offences Act, 2012.

ii) Cyber Bullying: It is an act of bullying committed through various online and social media platforms available on the internet. Anyone can be a victim of this kind of bullying, but the most suffered group includes teenagers. However, at times perpetrators have also been identified to be a child which is quite distressing as this may be seen to be a trivial issue but this may act as a stepping stone for a child in the domain of criminal world.

Even though this issue is severe and sensitive in nature, Parliament has not enacted a clear law on this subject. Earlier, by way of an amendment in the year 2000, Section 66A was inserted in the Information Technology Act, 2000 which penalized cyber bullying, however it was declared unconstitutional by the Hon'ble Supreme Court in the case of *Shreya Singhal v. Union of India*[22] as being violative of freedom of speech and expression and Section 66A not fulfilling the criteria as set under Article 19(2) of the Constitution to curtail the fundamental right.

Even though the cases pertaining to cyber bullying may be prosecuted under any other general law on fulfillment of set criteria for the required offence, there has been a lack of specific law after striking down of Section 66A, the result of which has been suffering of genuine victims.[23]

Instance of misuse of above laws

[19] Rodney D. Ryder & Nikhil Naren, Internet Law Regulating Cyberspace and Emerging Technologies, 4.32 (2020).

[20] The Indian Penal Code, § 354D (1860).

[21] The Indian Penal Code, § 10 (1860) provides an exhaustive definition of 'Man' and 'Woman' and only includes man and woman of any age respectively.

[22] Writ Petition (Criminal) No. 167 of 2012.

[23] NS Nappinai, Technology Laws Decoded, 191 (2017).

Even when these provisions has been enacted for the protection of the victims, there arises few cases in which Courts have recognized the misuse of the above-mentioned provisions. In one such instance, an FIR was filed against a person for capturing a picture of a child witness in the police station. The Hon'ble Kerala High Court in the given case quashed the proceeding initiated under Section 66E of the IT Act, 2000 as quite apparently the above act did not fulfill the criteria of capturing an image of the private area of the child.[24]

The Juvenile Justice (Care and Protection of Children) Act, 2015

This Act categories child into two broad categories- child in conflict with law and child in need of care and protection and with the help of this classification, legislators have tried to provide protection to both the child victim as well as to a juvenile.

Even when a juvenile is apprehended to have committed an offence and placed in the custody of the concerned authority, the Act imposes duty upon such person in charge of the child to act as his parent. Further, bail has been made a rule for such child in conflict with law unless it is proved that he is associated with a known criminal.[25] Even when a child is convicted, the punishment includes release after advice or admonition, group counselling, community service, fine on parents, release on probation of good conduct and to be sent to a special home for period not exceeding three years.[26] This has been done to reduce the stigma attached to a convict to the lowest possible standard so that a child can again re-integrate himself into the society.

The Act also provides specific protection for child in need of care and protection and this terminology not only includes victims of any offence but also includes those children who are not victims to any offence but need care and protection.[27] This Act authorizes the Child Welfare Committee to restore such child in the lawful and fit person with or without the supervision of Child Welfare Officer, or, places a child in Children's Home, or, may pass Foster Care orders and Sponsorship orders[28] depending upon the facts and circumstances of the case.

Government Advisories

In light of involvement of children in cyber offences, Ministry of Home Affairs has issued advisories to combat this issue, some of them can be listed as:[29]

i) Special Training for the law enforcement agencies including of police, prosecution and judges in order to sensitize them about the juvenile justice and human rights.

ii) Setting up of exclusive children desks in each police station with a clear mandate on compulsory registration of FIR in matters pertaining to children.

iii) Speedy investigation should be conducted and chargesheet shall be filed with three months.

iv) Services of Professional Counsellors should be provided to the victims for their rehabilitation.

v) General awareness regarding the special legislations pertaining to child should be improved among

[24] Lakshmi Prathapan v. State of Kerala, Criminal Miscellaneous No. 4776 of 2014.

[25] The Juvenile Justice (Care and Protection of Children) Act, § 12 (2015).

[26] The Juvenile Justice (Care and Protection of Children) Act, § 18 (2015).

[27] The Juvenile Justice (Care and Protection of Children) Act, § 2(14) (2015).

[28] The Juvenile Justice (Care and Protection of Children) Act, § 17 (2015).

[29] F. NO.15011/48/2006-SC/ST-W, Ministry of Home Affairs, Government of India (14th July 2010).

members of society.

vi) Overall safety conditions in schools, educational institutions, public transport used by the children shall be improved.

Central Government has established Indian Cyber Crime Coordination Centre in order to handle cyber offences in coordinated manner with all the involved agencies in a matter.[30] Central Government has also initiated a Toll Free Number and National Cyber Crime Reporting Portal to report every kind of cyber offences committed against child in order to strengthen the existing law enforcement framework and for efficient handling of such offences.[31]

CONCLUSION AND SUGGESTION

Anything and everything related to child remains a sensitive issue and so is the involvement of child with the cyberspace. Not only sensitive, it is also a complex issue due to ever evolving nature of the cyberspace. Hence, the regulation of interaction of a child with the cyberspace is of paramount importance, and, apart from legislative measures, government shall also provide Circulars and Advisories to the relevant law enforcement agencies as and when required.

Before concluding, the researcher would like to put forward few suggestions, in addition to the implementation of Central Government's advisories in the spirit and the letter, which are:

- Cyber Sensitization programs shall be run in government and private schools explaining to children at early age the very nuances of ill-effect of indulging in cyber offences on their own psychological condition as well as that of the victim

- Cyber Wellness Programs should be run in the community catering to the victims as well as to the juveniles so that they do not get victimized from or get involved in any cyber offences.
- Awareness programs about how to avoid becoming a victim and why not to indulge in cyber offences should be run through print and electronic media by the state governments as well as central government.
- Government shall promote Model Net Etiquettes in print as well as electronic media and for the same, help of celebrated public figures can also be taken.
- Government may also collaborate with the concerned NGOs to functionalize above suggested programs.
- There shall also be an increase in the Cyber Desks at the police station to increase the accessibility of the law enforcement agencies.

[30] Steps Taken to Deal with Cyber Crime and Cyber Security (17 JUL 2019) *available at* https://pib.gov.in/Pressreleaseshare.aspx?PRID=1579226.

[31] Steps taken for the Cyber Safety of Women and Children (22 JUL 2021) *available at* https://pib.gov.in/PressReleasePage.aspx?PRID=1737762.

4

RIGHT TO PRIVACY IN CYBERSPACE

KEYWORDS

CYBERSPACE, RIGHT TO PRIVACY, INDIVIDUAL, DATA, CRIMES, INFORMATION AND TECHNOLOGY.

CHAPTER FOUR

RIGHT TO PRIVACY IN CYBERSPACE

AUTHORS

AMISHA RERRU SINGH, LL.M STUDENT (CORPORATE AND COMMERCIAL LAW), SCHOOL OF LAW, SHARDA UNIVERSITY, INDIA

DR RITU GAUTAM, ASSISTANT PROFESSOR, SCHOOL OF LAW, SHARDA UNIVERSITY, INDIA

ABSTRACT

Cyber privacy is a disputed and unsettled issue in legal jurisprudence around the globe. The power of the new slogan, termed 'Information Technology,' has engulfed the present cosmos in the modern era. Individual privacy has risen to the forefront of the Jurisprudential conscience as a result of the sempiternity of knowledge in the midst of the 'Information and Communication Technology Revolution.' Even while the general population lives and transacts as effortlessly online as they do offline, people are not regulated or held by any standards in cyberspace. As more of our regular lifestyle shift online, aided in large part by the ongoing COVID-19 pandemic and quickly evolving technology, we must consider what cyber-protections we have readily accessible and the corresponding standards of protection of our valuable data. It is questionable to what extent residents of democratic countries would be prepared to provide as well as at the same time protect sensitive information. However, it is the legal domain's job to develop an appropriate policy for protecting online privacy from cyber spying, cyberstalking, corporate espionage, devastating cyber-attacks, and website de-

facement.

As a corollary, the researcher in this research paper tries to find out likely outcomes to assess those things that can be useful for our legislature to get an opportunity to construct a concrete base for setting standards, enacting guidelines, and conducting further research related to the evolving technology era's possible problems and solutions regarding right to privacy. Moreover, this research paper places reliance on the Constitutional Right to Privacy vis-à-vis the arena of cyberspace.

MEANING OF CONSTITUTIONAL RIGHT TO PRIVACY

When somebody comes across its meaning, the concepts privacy and confidentiality are abstract. It has been used in a variety of ways in various situations and circumstances. According to **Black Law Dictionary**, "the right to privacy" is a "collective term covering multiple rights recognized to be inherent in the concept of ordered liberty, and such rights protect individuals' freedoms to make fundamental choices involving themselves, their families, and their relationships with others."

The legitimate claim of an individual to select the amount to which he desires to share oneself with others, as well as his choice of information about the time, place, and circumstances in which he communicates with others, has been described as privacy in a general sense. It refers to his ability to retreat or participate in any way he thinks fit. It also refers to an individual's right to govern the transmission of personal information since it is his chattel.

Right to privacy, on the other hand, refers to a man's right to be left alone and to be devoid of undesired publicity. The term "right to privacy" is a general term that incorporates a number of rights that are acknowledged as inherent in the concept of organized liberty in the modern era. The right to personal liberty, as well as the ability to travel and speak, all contributes to the right to privacy.

"Privacy postulates the reservation of a private space for the individual, described as the right to be left alone," according to Dr. D.Y. Chandrachud. The individual's autonomy lies at the heart of the concept. The concept of privacy allows an individual to establish and govern the human element that is inextricably linked to their identity. The primary factor in determining the areas of personal importance exemplifies the inviolable quality of the human psyche. Individual autonomy is related with issues that can be kept hidden as well depending on the liberty an individual is subject. These are concerns about which a reasonable expectation of privacy exists.

The mind and body are inextricably linked in the human consciousness. The body's integrity and the mind's sanctity can only exist if each individual has the unalienable ability and right to protect a private space in which the human individuality can grow. The personality's inviolability would be questioned if it lacked judgment in making a trait.

Acknowledging a personal space is just acknowledging that each person has the right to plan and explore their own path of personality development. As a result, privacy is a tenet of human dignity. Thoughts and behavioural patterns that are personal to an individual are privileged to a private space devoid of social pressures. A human is not assessed by others in that sphere of solitude. Individual privacy allows each person to make important decisions that are reflected in their personality. It allows people to hold on to own views, thoughts, expressions, ideas, philosophies, preferences, and choices in the face of societal homogeneity expectations.

"Privacy is an inherent affirmation of variance, of the individual's right to be distinct and to create a solitary zone in defiance of the tide of similarity. Privacy shields a person from the prying eyes of the public in concepts that are personal to him or her. Privacy pertains to the individual rather than the location with which they are affiliated. Because the person can select how liberty is best enjoyed in privacy, privacy is the cornerstone of all liberty. Individual dignity and privacy are closely interwoven in a pattern of the fabric comprising of a multiple civilization forming a thread of diversity."

Right to Privacy in the Realm of Cyberspace and its Significance

The current world order specifies two kinds of privacy. The first is privacy in the real life, which can be defined as minimized level of intrusion into one's physical space or solitude; the second is privacy in the virtual environment, also known as cyber space, which refers to the collecting of user information from a multitude of sources, including the internet. Information collecting, processing, publication, and breach of private data are all examples of privacy and its corresponding aspects in the virtual world.

People appear to be more immersed in the digital world, also known as cyber world, as a result of rapid technology breakthroughs and rising internet use. Platforms like Facebook and Twitter are helping to facilitate this addiction to a greater level. Websites like Facebook, Twitter, Instagram, and YouTube have nearly two billion active users and offer applications and features including communication, photo and video posting, and sharing. These websites collect, store, and process a large amount of personal information on their databases, which are frequently located outside of India's territorial jurisdiction. Theft or security breaches of this data by a third party pose a little and sometimes a wide-ranging risk to an Indian subscriber of these websites.

The Information Technology Act, which was particularly intended to offer legal status to e-commerce in India, is vague on these corporations' liability with regards to third-party use of this data without the user's consent. The act makes no use of the phrase "cybercrime." Some scholars refer to this Act as "toothless law" because of its ineffectiveness in enforcing punishments or repercussions against those who chose to abuse cyberspace's coverage. As a result, there is a legal vacuum that must be filled as soon as possible.

Digital Footprint

Every netizen leaves a digital footprint (a digital trace of data created by a person while using the internet.) This comprises web pages visited, emails exchanged, and information supplied online. When someone uses the internet, certain information is compiled at times, even without the person's knowledge. As a result, digital footprints can be grouped into two categories i.e. Active and Passive digital footprint.

When we talk about active digital footprint it comprises of publically identifiable data that you communicate on the web, such as data submitted on Facebook, Instagram, or other social platforms, as well as any other information that the individual keeps posting for personal activity. The data that a private corporation accumulates behind the curtains or veils of technology, such as IP address, transaction information, navigation details, and location so on, is known as a passive digital footprint.

This digital footprint, along with many other users' data, is now recurrently used by companies alone without user's prior consent to identify and detect habits of a user's behaviour; however, this data is also used by a private person to commit illegitimate or immoral acts, such as morphing, which was the most common cybercrime against women just few years ago, in which publicly available photographs of females were transformed to offensive pictures thereby breaching privacy.

The Facebook-Cambridge analytica scandal, which involved the collection of 50 million of the subscribers' Facebook profile data through the use of a third-party application called "this is your digital life," which tempered with Facebook login, was the worst data exploitation event of all period in 2017. Cambridge analytica used this information to try to sway public sentiments of various political organizations.

Technological has a nasty aspect since it makes commercial activities easier. Normally, the law keeps up with technological advancements, but the rate of technological advancements in recent years, particularly in the sphere of information and technology, has made it impossible for the legal system to stay up. Modernizing penal laws in many nations that predate the invention of computers is a major concern. On the one hand, current laws must be changed to address device criminality such as hacking, deliberate fabrication or elimination of data, technology theft, software threats, and so on; on the other hand, new legislation is required to safeguard data security and piracy.

LAWS GOVERNING DATA PRIVACY TILL DATE

There is currently no explicit legislation in India addressing data protection or privacy. The Information Technology Act, 2000 and the Contract Act, 1872 are the important data protection statutes in India presently. In India, a standardized data protection law is expected to be enacted in the coming years. The Information Technology Act, 2000 investigates complaints relating to civil compensation and criminal penalties for improper revelation and exploitation of personal data, as well as breaches of contractual agreements pertaining to personal data.

A body corporate that is in possession, dealing, or handling any sensitive personal data or information, and is negligent in implementing and maintaining reasonable security practices, resulting in wrongful loss or wrongful gain to any person, may be held liable to pay damages to the person so affected under *section 43A of the Information Technology Act, 2000*. It is crucial to highlight that the reimbursement that can then be requested by the harmed party in such instances has no maximum limit fixed under the statute but governed by the rule of damages under the Contract Act.

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, have indeed been enacted further to strengthen the regime of data privacy. The Guidelines only cover the safeguarding of "vulnerable private and confidential information/data of a person," which includes a range of comprehensive definitions such as:

"Password, financial information (such as bank account/credit card/debit card/other payment instrument) details, Physical, physiological and mental health conditions, Sexual orientation, Medical records and history, Biometric information."

According to *section 72A* of the IT Act, 2000, which states that if a person knowingly and intentionally disclosing information without the consent of the person concerned and in violation of a legitimate contract is punished up to three years imprisonment and a fine of up to Rs 5,00,000.

It should be acknowledged that *section 69* of the Act, which is an exception rather than the basic policy/rule of maintaining private data and secrecy, provides that where the Government is satisfied that it is essential as to the function of India's sovereignty, defensive tactics, safety, cordial relations with foreign entities, or public order, or for blocking incitement to the commission of any cognizable offence pertaining to the above, or for any investigative purposes, the Government may disclose details as and when required.

However, in the 52nd Report on Cyber Security and Right to Privacy, the Parliamentary Standing Committee on Information Technology stated that an extreme rise in cyberspace activities and access to the connectivity in India, coupled with a lack of user end discipline, inadequate computer system protection, and the possibility of unidentified use of ICT allowing users to impersonate and cover their criminal trends, has empowered more users to experiment with ICT abuse for nefarious purposes. This component, according to the Committee, has a substantial impact on neutralizing the deterrent effect established by the legal structure, which is not aptly recognized by the IT Act, 2000 and related statutes.

The statute was amended in 2008, particularly known as the Information Technology Amendment Act, 2008 which incorporated several safeguards to protect a person's privacy from internet intrusion and exploitation. It includes fines and prison sentences for hacking (Sections 43, 66), three years in prison for privacy violations (Section 66E), identity theft (Section 66 C), and cheating by impersonation (Section 66 D), and abusive email (Section 66 E); (Section 66A).

Unauthorized disclosure of personal information by someone who obtained it through a legitimate contract and without the consent of the person to whom it belonged or was stolen is punishable under Section 72A of the IT Act. A well sorted example of the same is GDPR which was successfully formed by the European Council (EU) in 2018 and is among the most rigorous laws to protect the personal data of European Union citizens. This policy has proven to be a significant step forward in the realm of privacy shield. The introduction of this policy has had a significant influence on different tech corporations such as Google, Facebook, and many other prominent e-commerce sites. This rule has undoubtedly established new jurisprudence in the field of cyber law.

Case Laws

In the case of **Amar Singh v. Union of India,** the Supreme Court addressed the right to privacy in the context of phone call monitoring and recognized the same as an integral part of individual's privacy. Similarly, in the **People's Union case,** the question of whether surveillance of telephonic messages/tapping of telephonic conversations constituted a significant infringement of an individual's right to privacy was reviewed in detail by the Hon'ble Apex Court, which decided as follows:

"17. We have no problem in holding that the right to privacy is established in Article 21 of the Constitution as part of the right to "life" and "personal liberty." When the facts of a case give rise to a right to privacy, Article 21 is invoked. The said right cannot be restricted "unless in accordance with legal procedures."

"18. The right to privacy — by itself — has not been identified under the Constitution. As a concept it may be too broad and moralistic to define it judicially. Whether right to privacy can be claimed or has been infringed in a given case would depend on the facts of the said case. But the right to hold a telephone conversation in the privacy of one's home or office without interference can certainly be claimed as "right to privacy"."

Telephonic conversations are frequently personal and private. Thus, telephone is an integral component of contemporary man's life. It is regarded as so vital that an increasing number of people keep mobile telephone equipment in their wallets. A man's private life revolves around his telephonic conversations. These telephone conversations in the privacy of one's house or apartment are unquestionably protected by the right to privacy. Eavesdropping, then, on such conversations would be a violation of Article 21 of the Indian Constitution unless otherwise approved by law.

Furthermore, in the case of **Vinit Kumar vs. Central Bureau of Investigations and Ors,** the Bombay High court upheld, *"the constitutionality of breach of confidentiality with reference to small and minute details like wiring, equipments and the requirement of taping phone calls for surveillance purpose only for occurrences that fall under the umbrella of public emergency or the interest of national security."*

In **Indian Hotel and Restaurant Association (AHAR) v. The State of Maharashtra,** the Supreme Court regarded that the data kept in CCTV footage to be a person's private information, citing Puttaswamy's decision in support. *"Comprehensive surveillance of actions inside the territory of dance bars by CCTV cameras is excessive and disproportionate, the court said. Monitoring, storing, and retaining dance performances are an unjustified breach of privacy that could possibly put women bar dancers in danger. Because CCTV footage is a reliable source for identifying a person that becomes part of his personal information, triggering his right to privacy."*

Innovation and Technology now has the potential to increase massive data sets that may have been statistically analyzed to show patterns, tendencies, and relationships, particularly in the context of human behavior and interactions around the world. According to the council on Free and Fair Digital Economy's report, *"Data gathering procedures are frequently opaque, bogged in complex privacy forms that are unintelligible, thereby leading to practices that users have little influence over."*

CURRENT LEGAL DEVELOPMENTS UNDER DATA PRIVACY LAWS IN INDIA

The Ministry of Electronics and Information launched the PDP Bill in the Indian Parliament on December

11, 2019, and it is primarily based upon the GDPR Model currently put into operation in the European Union. On November 22, 2021, a joint parliamentary committee reviewed and endorsed a modified application of the PDP Bill. The privacy information by the Govt., enterprises, and global firms will be governed by this prospective statute.

Personal data can be described as *"...data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute, or other feature of such natural person's identity, whether online or offline, or any combination of such features with any other information, and shall include any inference drawn from such data for the purpose of profiling...".*

The construction of a Data Protection Authority (DPA), comparable to that of the European Union, including the segmentation of personal data which also need to be protected, is one of the far more interesting advances proposed under the PDP Bill. The PDP Bill, for example, uses a three-tiered framework to guarantee data security and localization. Personal data is exempt from data transmission limitations; nevertheless, "sensitive personal data" and "important personal data" are subject to restriction as stated by the central government.

Quantitative statements, personally identifiable information, caste, religion or political convictions, or any other genre of data determined by the Indian government, in collaboration with the DPA and the appropriate sector-specific regulator, is considered sensitive personal data in consonance with the PDP Bill. Furthermore, "essential personal data" is not allowed to be sent outside of India in any circumstance except as those necessitated by the government. Data transmissions to countries or organizations which are priorly judged so as to provide an assurance of safety are permitted to a limited degree.

In contrast, the PDP Bill mandates a series of criteria on data controllers (including social networking middlemen) in terms of how they receive, manage with/process, and keep personal data. It holds them responsible for abiding to the requirements of a complete series to the transfer of personal information carried out by it or on its account. Data fiduciaries, for example, are responsible for putting in place methods for age verification and parental authorization whenever managing highly sensitive data concerning children.

In addition, processing or transferring data in defiance of the PDP Bill carries harsh penalties. An infringement under the PDP Bill seems to have a maximum pecuniary penalty of INR 15 crore. The DPA also makes processing of de-identified private information without approval illegal by up to three years imprisonment, and fine, or both. The PDP Bill proposes to create an appellate body to hear first-round appeals against the DPA's judgment, with a second-round appeal presented to the Supreme Court of India.

CONCLUSION

A person's existence has now significantly grown in the electronic dimension known as the cyber world as a result of changing times urging for a need to switch to the virtual world on one hand and heavy emphasis on technology and the internet on the other. This exposure has the potential to endanger a person's physical life and obstruct fulfilment of his rights. An Individuals' virtual privacy must be recognized and protected as soon as possible to protect them from large scale harm. The European Union's General Data Protection Regulations contain rigorous and systematic rules and will serve as a model for future data protection legislation in India.

The Personal Data Protection Bill has a multitude of conformity procedures in it, so it could be a good place to start when it comes to regulating corporations that hold user data in India. In addition, the Act establishes a penalty structure to function as a disincentive where non-compliance occurs. Economic and commercial interests, as well as the authenticity of a person's virtual existence, should be considered while assessing these compliance and sanctions. Other nations' legislations on the other hand inculcate the mechanism, particularly on the subject of cross-border data transfers, and the same should be examined in order to make the law more consistent and interoperable.

Yet there is a good argument to be made in justification of the PDP Bill, it can also be asserted that the Government of India has evolved from inadequate monitoring of cyber and data security in India to developing an effective system for the same. Many adversaries have voiced doubts about the Indian government's overstepping powers under the PDP Bill, such as the ability to legislate what qualifies essential personal data, and furthermore many international firms believe the planned reforms are too stringent to comply with. Although the Indian government is inclined to adopt the bipartisan parliamentary committee's proposal of the PDP Bill, whereby a number of key concerns about data security in India are required to be addressed.

Not just for the common Indian person, but also for the sovereignty of the nation, the enforcement tactics stated above are vital. Given the foregoing, it is reasonable to conclude that, whilst the IT Act and its additional policies, rules, and norms have evolved and progressed since their establishment, they are insufficient to ensure data security and safeguard against cyber dangers.

REFERENCES

1. Arun Sharma, Personal Data Protection Bill can seed uncertainity for businesses, The Economic Times | Rise, (Feb. 2, 2022, 4:19 PM), https://m.economictimes.com/small-biz/policy-trends/personal-data-protection-bill-can-seed-uncertainty-for-businesses-reduce-competitiveness/articleshow/88116148.cms.
2. Suneeth Katarki, Namita Vishwanath, Ivana Chatterjee, Rithika Reddy Varanasi, India: The Personal Data Protection Bill, 2019 – Mondaq, Mondaq, (Feb. 3, 2022, 8:09 PM), https://www.mondaq.com/india/privacy-protection/880200/the-personal-data-protection-bill-2019-key-changes-and-analysis.
3. Supratim Chakraborty, India: Data Protection Laws and Regulations 2021, ICLG India, (Feb.4, 2022, 4:28 PM), https://iclg.com/practice-areas/data-protection-laws-and-regulations/india.
4. Supra note 32. Arun Sharma, Personal Data Protection Bill can seed uncertainity for businesses, The Economic Times | Rise, (Feb. 2, 2022, 4:19 PM), https://m.economictimes.com/small-biz/policy-trends/personal-data-protection-bill-can-seed-uncertainty-for-businesses-reduce-competitiveness/articleshow/88116148.cms.
5. Suneeth Katarki, Namita Vishwanath, Ivana Chatterjee, Rithika Reddy Varanasi, India: The Personal

Data Protection Bill, 2019 – Mondaq, Mondaq, (Feb. 3, 2022, 8:09 PM), https://www.mondaq.com/india/privacy-protection/880200/the

6. Gautam, R., Kulshrestha, P., & Goswami, M. A. K. (2021). Mediation And Family Dispute Resolution Mechanism: A Case Study On Clinical Legal Education. Elementary Education Online, 20(3), 2490-2490.
7. Gautam, R., "Proliferation of Cyber Crime and Indian legal system with special reference to Gwalior Division" Available at: https://shodhganga.inflibnet.ac.in/handle/10603/250817 Retrieved on: 22/07/2021
8. Pandey, N., Gautam, R., "property right of women in patriarchal indian society: a comprehensive study on legal narrative" Available at: https://www.researchgate.net/publication/361733554_PROPERTY_RIGHT_OF_WOMEN_IN_PATRIARCHAL_INDIAN_SOCIETY_A_COMPREHENSIVE_STUDY_ON_LEGAL_NARRATIVE_PROPERTY_RIGHT_OF_WOMEN_IN_PATRIARCHAL_INDIAN_SOCIETY_A_COMPREHENSIVE_STUDY_ON_LEGAL_NARRATIVE
9. Gautam, R., Medical health condition of prisoners and discrepancy in facilities among the states of Uttar Pradesh, Haryana and Delhi, International Journal of Health Sciences Follow journal, DOI: 10.53730/ijhs.v6nS6.12256
10. Gautam, R., Kanpur Philosophers ISSN 2348-8301 Vol IX, Issue V (IV), 2022151EFFICACY OF PROCEEDINGS OF CONCILIATION AND SETTLEMENT OF ANINDUSTRIAL DISPUTE UNDER INDUSTRIAL DISPUTES ACT, 1947, A CRITICAL Analysis. Available from: https://www.researchgate.net/publication/361733673_Kanpur_Philosophers_ISSN [accessed Sep 11 2022].
11. Elonnai Hickok, CIS Welcomes 52nd Report on Cyber Crime, Cyber Security and Right to Privacy, CIS India, (Jan. 28, 2022, 3:22 PM), https://cis-india.org/internet-governance/blog/cis-welcomes-fifty-second-report-on-cyber-crime-cyber-security-right-to-privacy.
12. The Information Technology Act, 2008, Ministry of Law, Justice and Company's Affairs, (Legislative Department), (Jan. 29, 2022, 6:18 PM), https://police.py.gov.in/Information%20Technology%20Act%202000%20-%202008%20(amendment).pdf.
13. Gautam, Ritu, Cybercrimes and International legal regime, Available at: https://shodhganga.inflibnet.ac.in/bitstream/10603/250817/10/10_chapter-iv%20%20cybercrime%20issues%20and%20international%20legal%20regime.pdf
14. Gautam, Ritu, Cyber crime in India, Available at: http://hdl.handle.net/10603/250817
15. Indian Hotels and Restaurant Association vs. State of Maharashtra, 2019 (3) SCC 429.
16. PRS Legislative Research, A free and fair Digital Economy, Committee Reports, PRS India, (Feb. 1, 2022, 10:00 PM), https://prsindia.org/policy/report-summaries/free-and-fair-digital-economy.
17. PRS Legislative Research, The Personal Data Personal Bill, 2019, PRS India, (Feb. 2, 2022, 7:09 M), https://prsindia.org/billtrack/the-personal-data-protection-bill-2019.

5

INDIA’S CYBERCRIME, CYBERSECURITY AND CYBER REGULATION

KEYWORDS

INSURANCE, INFORMATION TECHNOLOGY ACT, AND ETHICAL HACKING

CHAPTER FIVE

INDIA’S CYBERCRIME, CYBERSECURITY AND CYBER REGULATION

AUTHORS

AVINASH KRISHNA GOSWAMI, RESEARCH SCHOLAR, SCHOOL OF LAW, SHARDA UNIVERSITY, INDIA

DR. RITU GAUTAM, ASSISTANT PROFESSOR, SCHOOL OF LAW, SHARDA UNIVERSITY, INDIA

ABSTRACT

Each moment, one person in India becomes an internet user. With its combination with meticulously maintained stages and apparatuses, sheltering guardians and understudies from cybercrime is proving to be a difficult undertaking. However, the underlying reality is that internet users are not being updated on helpless digital hazards and security difficulties at the rate at which they are being updated through the usage of web-enabled instruments and apps. Thus, the focus of the momentum study article is on determining the answers to troubling questions such as “Is the Netizen actually aware that he or she is defenceless against various Digital wrongdoings?” and “Assuming the netizen is aware, how much?” “If individuals are not cognizant of cybercrime, what actions may be implemented to make them more cognizant and refreshed?” The article recommended a theoretical approach for sustaining and implementing meditation programs among internet users in relation to cybercrime.

INTRODUCTION

The world is no longer ruled by guns, oil, or money; it is ruled by ones and zeroes—small bits of information. It is entirely composed of electrons. There is a battle that exists apart from the global conflict. There is no reason to be concerned about who possesses the most BULLETS. It is a means of deciding who holds the data. What we see and listen, how we operate, and what we see are all dependent on data or data.

There are no statements that more accurately describe the current state of technology than those spoken above by universe the low life scum in the film "sneaker."

Cybercrime is defined as illegal behavior committed via the use of a computer or the Internet. Cybercrime include charge card and checkbook fraud, programming heists, copyright infringement, tracking, and provocation. Malicious software (malware) is frequently disguised in seemingly harmless email communications. Phishing scams are designed to deceive Internet users into disclosing their passwords and other sensitive information. Cybercrime can be committed against persons, property, or organizations. Persistent monitoring of PC connections is critical for the protection of sensitive data. Digital wrongdoings or cybercrime directed against individuals include spam and satirical email, as well as criticism, badgering, and following. A farce communication is one that has all the hallmarks of being sent by a source other than the true author. Spam email is a collection of several duplicates of a single email, such as garbage messages or offer requests. When someone publishes false allegations on a website or by email, this is considered digital maligning. Digital following occurs when someone uses chat rooms, email, and long-distance informal conversation to monitor another person's Internet activity and engage in unwelcome contact.

Cybercrime or digital misbehavior against property includes charge card fraud, programming robbery, and transmission capacity burglary. By linking malware to email, cybercriminals obtain credit card information. Phishing is a technique used to fool a person into providing personal information. Phishing emails and websites can appear to be legitimate. They may bear the authorization logo of a financial institution. Transmission capacity thievery is unauthorised membership in an Internet organisation. Programming theft is the act of copying and disseminating protected software. Sharing "breaks" and key generators for the purpose of circumventing software assurance is considered programming theft.

Determined hazards are advancing clandestine assaults against an organization. Government offices are frequently the target of this type of digital malfeasance. Digital hoodlums frequently contact a guarded information organization or workplace location for an extended period of time before being discovered.

During this time period, the digital thief approaches confidential data. Digital hoodlums employ specially crafted PC malware to retrieve data that has been blocked by firewalls. Constant dangers have evolved to include many governments and political organizations engaged in clandestine actions.

"Hacktivism is a recent development in the field of Internet security.

Hacktivism is a kind of digital activism used to express dissatisfaction or to gather data for use by a group opposed to the target site. Hacktivists gain access to private or governmental data sets and websites in order to get classified information or cause havoc on the site. Hacktivists may shut down a website in opposition to a government policy or commercial initiative. Sites may be appropriated to further a social or political agenda. Hacktivists are often efficient and possess the necessary high-level coding ability to obtain sensitive data".

The consequences of PC misbehavior are massive in terms of financial costs and human security. Due to the numerous advantages provided by the web, criminals are encouraged to report the following types of wrongdoing: -

- Intentional wrongdoing or cyber-influence of others.
- Economic misbehavior as a result of wrongdoing or cyber-influence.
- Improper conduct or cyber-influence on public safety.
- Unrestricted innovation licenses.

There are two distinct types of criminal liability. The first is beyond a reasonable doubt exercise. Through PC programming, digital infractions are perpetrated on the distant company. Digital wrongdoings have an effect on a wide range of administrations. Not only company owners, but also consumers are severely hurt by digital crimes.

Although the word "web extortion" is quite broad, it has not been defined specifically in the showcase Information Technology 2000. The fakes on the web will use a variety of structures in their grouping, making it difficult to keep up with them. However, the primary purpose of this investigation is to ascertain the security status and to ascertain which issues should have been addressed earnestly with regards to exchange security, protection, banking extortion, and property, among other things. Each passing day brought fresh developments in the field of personal computer innovation. Fresher-capacity PCs have been designed. These PCs are incredibly fast and have no upper limit. They currently fill a variety of roles. As a consequence, many firms purchased their own PCs rather than relying on bureaux, and as a result, various bureaux began to improve, regularly expanded into the programming area, or sought specialist markets.

HISTORY OF CYBER CRIMES

"The first reported instance of digital misbehavior happened in 1820! That is unsurprising given the fact that the math instrument, which is believed to be the first kind of a computer, has existed in India, Japan, and China since roughly 3500 B.C. However, the era of modern personal computers began with Charles Babbage's scientific motor".

"The loom was delivered in 1820 by Joseph-Marie Jacquard, a French material manufacturer. This device allowed for the repetition of a sequence of stages in the wrapping around of unique textures. This caused fear in the representatives of Jacquard that their typical work and vocation would be jeopardized. They offered evidence of deceit in an attempt to dissuade Jacquard from expanding its use of the new technology. This is the first instance of digital crime that has been documented".

"Digital misconduct is a pernicious practice that has its origins in modern life's growing reliance on personal computers. In an age where everything from microwave and freezers to thermal power stations is managed by personal computers, digital malfeasance has been predicted to have pretty heinous consequences. Significant online wrongdoings in the recent past include the Citibank heist. US$ ten million were fraudulently transferred from the bank to a Swiss financial balance. The assault was carried out by a group of Russian programmers led by Vladimir Kevin, a well-known programmer. The gathering put the bank's security frameworks at risk. Vladimir was allegedly breaking into Citibank computers using his business PC at AO Saturn, a computer firm in St. Petersburg, Russia. He was apprehended on his way to Switzerland at Heathrow airport.

RELEVANCY OF CYBER CRIMES

This day and era, there has been a great increase in the usage of the Web or internet in every sector of society, and as a result of this increase in use, several new wrongdoings have occurred. Such crimes involving the use of personal computers in conjunction with the use of the Internet are sometimes referred to as Cyber Crimes.

In any event, in Indian law, the term "cybercrime" has not been defined. In India, one regulation that addresses the charges associated with such infractions is the Information Technology Act, 2000, which was amended in 2008 by the IT Amendment Act. In any event, these two key rules expressly prohibit the use of the term "cybercrime." When common sense is examined, it is not easy to describe this concept.

To define such an incident, it is a mixture of transgression and PC. Thus, when a computer is used to commit an act, this is referred to as "digital crime."

PC is defined broadly in our Indian Information Technology Act 2000 as – PC means any electronic attractive, optical, or other high-speed data handling gadget or framework that performs consistent, numeric, and memory capacities through electronic, attractive, or optical motivating factors, and integrates all input, yield, managing, capacity, PC programming, or communications offices that are affiliated or connected with the PC in a logical manner. The relevance of digital malfeasance is fundamentally different from the significance of traditional wrongdoing. Both integrate lead, whether by act or oversight, that results in a regulation of regulatory regulations and undermines the state's authority. Prior to evaluating the significance of digital misbehavior, it is necessary to study traditional crime.

"Wrongdoing is a social and financial anomaly that dates back almost as far as human society," "digital wrongdoing may be assumed to be those sorts of misconduct in which the PC is either an article or a subject of the direct constituting wrongdoing." "Any lawbreaker conduct that makes use of a computer, whether as a tool, a target, or a means of committing more violations, falls under the scope of digital crime."

That is to say, infractions committed via a computer are referred to as digital wrongdoings; they are also illegal whether committed in a network environment or on the web. In this instance, any anyone who commits a digital infraction is referred to as a digital crook.

The digital lawbreakers may be children and adolescents aged 6-18 years. It is possible that they are skilled programmers or strategists, con artists or mystical individuals.

It has become into a global worry in recent years as our reliance on personal computers has increased. Almost regularly, it has been reported that important areas have been seized or that an infection has damaged the framework; it is also employed to steal an individual's character. It is a type of misconduct that takes place over the internet. A virtual world created by humans via the use of personal computers and system administration.

"Digital wrongdoings are any infractions involving a personal computer or a network. Occasionally, the PC may have been used to do the violation, and in other instances, the PC may have been the victim of the crime".

"Digital wrongdoing encompasses any criminal conduct involving the management of personal computers and organizations, referred to as hacking. Additionally, digital misconduct typically includes offenses committed via the internet. For example, numerous wrongdoings such as selling and online extortion, fraud, and also charge card account thefts are considered digital wrongdoings when criminal activities are conducted out utilizing a computer and the internet." Digital wrongdoing is a new Species, a new form of hoodlum that is involved in disrupting business and bureaucratic interests.

The term "cyber wrongdoing" refers to all the activities carried out with illegal intent on the internet. Due to the mysterious nature of the internet, it is possible to become involved in a variety of crimes without fear of prosecution. People with insights have been horribly exploiting this section of the web to perpetrate online crimes. "Worldwide, digital misconduct is referred to as wrongdoing submitted over the web. It has developed into a major source of concern from one end of the world to the other in recent years. The concept of digital wrongdoer is similar to a new type of show misbehavior; if we look at online usage, we see that it isn't nearly as widespread as other other nations' wrongdoing; nonetheless, web-related wrongdoing is still in its infancy in this country. This is an exploratory review. To elicit pertinent information from purposefully chosen respondents, systemic corroboration (eye to eye contact and contextual analysis) was used. The examination uncovers that, while digital wrongdoing is not prevalent in the study location, responders are fooled at some moment by programmers, sexual entertainment locales, and web-based PC infection. It is steadily increasing consideration for the majority of the population in the research region".

Nobody truly owns the web, and no single man or organization controls it in its entirety. As a result, there is no centralized management in terms of inventive implementation or arrangements for usage and access. The terms web and World Wide Web WWW are widely used interchangeably in everyday speech; it is common to speak of "getting on the web" while running a program for viewing Web sites. However, the web is not inextricably linked to the World Wide Web".

NATURE OF CYBER CRIMES

This section provides some background information on PC wrongdoing, such as the types of PC wrongdoing that tend to occur most frequently and how they have been forestalled up to this point. In reality, PC misbehavior is altered, maybe significantly more than our specific definition suggests.

As a result, efforts to regulate it have varied as well. It appears to be self-evident, in light of episodic evidence, that extortion, child sexual entertainment, unauthorized access, and associated offenses account for the majority of PC misconduct". Digital misbehavior is a constant threat with an ever-changing face.

The electronic age has resulted in the development of a new type of abundance tracker. While their standard methods and gear may differ greatly from that of their heinous forefathers, their objective is essentially identical — expeditious acquisition at the expense of another.

Digital misbehavior is evolving, and not simply in terms of the criminal profile. Very unlike to what we have long believed to be the case, their inspiration and techniques have generated and are more current. What could be more heinous? As noted by the most recently released of the Symantec Security Report, organizations and individuals must be dynamic and responsive to safeguarding against assaults and foul-smelling code rule digital wrongdoing, and the focus has shifted away from the organization edge and toward Web browsers and Web services. Assailants are not typically constrained pockets of mostly befuddled individuals whose primary objective is to evaluate their skills against security standards or to methodically breach and mutilate sites.

Today, digital people who break the law are organized and, in the majority of cases, part of syndicates that are set up to create risks in order to separate data for the purpose of deception, coercion, and other lawbreaker activities. The general trend is characterized by an increase in weaknesses, and companies are pushed to address this problem across the framework.

Other reassuring facts included in the paper include Symantec. Having thwarted 1,5 billion phishing attempts, a 44 percent increase over the first half of 2005; and a daily average of 7,9 million extortion attempts - a 39 percent increase. Symantec has taken account of the following important directions in terms of hazard movement during the period of July to December 2005.

Incorporating innovations and framework should take fundamental business considerations into account and connect the roles of persons, cycles, and strategies. Is digital misconduct a myth or a reality? Nothing is improper until it is prohibited by regulation. Regardless, the vast majority of categories of digital misconduct remain outside the scope of regulation. Indeed, there is a dearth of consistent consensus. Above lines has attempted to define 'digital misconduct'. The study is conducted from a legitimate standpoint, and several perspectives are considered. A cursory examination has been made of whether digital misbehavior can be prosecuted within the present legal system or whether it requires an entirely new technique. This term has examined the functional technique for combating digital misbehavior and its conceivable troubles inside the conventional framework, which is based on a variety of norms that are largely ignored and difficult to administrate on the internet. The purpose of these analyses is to determine whether the general collection of laws is comparable to a roadster equipped with such technologically advanced culpability.

TYPES OF CYBERCRIME ATTACKS:

Cybercrime may manifest itself in a variety of ways. Here is a typical cybercrime attack mode.

- **Hacking**

It is a presentation of gaining unauthorized access to a computer system or organization.

- **Attack On Service Refusal**

The cybercriminal takes advantage of the victim's organization's transmission speed or floods their email account with infected email in this hack. The objective here is to wreak havoc on their routine administrations. Piracy in programming is the act of fraudulently replicating or misrepresenting actual work. Additionally, it encompasses the dispersal of goods intended to pass for the first.

- **Phishing**

Phishing is a tactic for illicitly obtaining classified data from bank/monetary institution record holders. It is an example of convincing one computer framework or organization to claim to have the character of another computer. It is typically utilized to acquire admission to organizations or PCs that provide limiting honors.

INSTRUMENTS OF CYBERCRIME:

There are several types of digital criminal devices.

1. **Linux distribution Kali**

   Offensive Security maintains and supports Kali Linux, an open-source operating system. It is a meticulously prepared automated legal sciences and infiltrate testing program.

2. **Ophcrack**

   This equipment is mostly used to decrypt hashes generated by comparable records of windows. It features a robust graphical user interface and the ability to operate on several stages.

3. **Encase**

   This tool enables an inspector to photograph and evaluate data on rigid circular and detachable plates.

4. **Secure Back**

   Safe Back is mostly used for scanning the hard plates of Intel-based personal computer foundations and re-establishing these images on a few different hard circles.

5. **Data unloader**

   This is a PC legal apparatus with an order line. It is free source and compatible with the Unix, which makes accurate plates suitable for automated legal scrutiny.

6. Md5sum

A gadget to examine enables you to determine whether or not information has been duplicated effectively to another capacity.

WORLD AND CYBER LAWS:

1. China's Great Firewall monitors the internet every second and prevents the spread of any hostile substance.
2. China has a veto over any content deemed hazardous or perilous to China's official authority.
3. Brazil is regarded as the greatest air airport in the world for hackers.
4. Iran is also a dangerous place for Netizens. Additionally, he has a Cyber Police squad dedicated to investigating misbehavior in Cyber Space.

CONCLUSION

To summarize, while a society free of wrongdoing is incredible and lives solely in deceit, there should be a continual effort of regulations to keep guilt to a minimum. Especially in a society that is more reliant on innovation, misbehaviour in light of electronic regulatory breaking will surely increase, and lawmakers will need to outperform everyone's expectations in comparison to the frauds in order to keep them under check.

Generally, innovation is a two-sided coin that may be used for either lucky or terrible purposes. Steganography, Trojan Horse, Scrounging (and even Dos or DDos) are essentially not infractions; nonetheless, when they enter into the hands of certain undesirable individuals with an illegal intent to use or abuse them, they fall into the category of digital misbehaviours and become chargeable offenses.

Thus, that should be the diligent efforts of rulers and lawmakers to ensure that innovation is implemented properly and is used for lawful and moral economic development, rather than for committing breaches. It should be the responsibility of the three partners, namely I) the leaders, controllers, administrators, and specialists; and II) the specialists. ii) Internet or Networking Service Providers, banks, and other arbiters, and iii) customers to manage data security by adopting their respective roles within the permitted constraints and ensuring compliance with the required norms.

REFERENCE

- M. Dasgupta, Cyber Crime in India- A Comparative Study (Eastern Law House, Lucknow, 2009)
- Yadav, D.S. Foundation of Information Technology, (New Age International Pub. Ltd. New Delhi, 3rd edn., 2007)
- Gautam, R., Kulshrestha, P., & Goswami, M. A. K. (2021). Mediation And Family Dispute Resolution Mechanism: A Case Study On Clinical Legal Education. Elementary Education Online, 20(3), 2490-2490.
- Gautam, R., "Proliferation of Cyber Crime and Indian legal system with special reference to Gwalior Division" Available at: https://shodhganga.inflibnet.ac.in/handle/10603/250817 Retrieved on: 22/07/2021
- Pandey, N., Gautam, R., "property right of women in patriarchal indian society: a comprehensive study on legal narrative" Available at: https://www.researchgate.net/publication/361733554_PROPERTY_RIGHT_OF_WOMEN_IN_PATRIARCHAL_INDIAN_SOCIETY_A_COMPREHENSIVE_STUDY_ON_LEGAL_NARRATIVE_PROPERTY_RIGHT_OF_WOMEN_IN_PATRIARCHAL_INDIAN_SOCIETY_A_COMPREHENSIVE_STUDY_ON_LEGAL_NARRATIVE
- Gautam, R., Medical health condition of prisoners and discrepancy in facilities among the states of Uttar Pradesh, Haryana and Delhi, International Journal of Health Sciences Follow journal, DOI: 10.53730/ijhs.v6nS6.12256
- Gautam, R., Kanpur Philosophers ISSN 2348-8301 Vol IX, Issue V (IV), 2022151EFFICACY OF PROCEEDINGS OF CONCILIATION AND SETTLEMENT OF ANINDUSTRIAL DISPUTE UNDER INDUSTRIAL DISPUTES ACT, 1947, A CRITICAL Analysis. Available from: https://www.researchgate.net/publication/361733673_Kanpur_Philosophers_ISSN [accessed Sep 11 2022].
- Gautam, Ritu, Cybercrimes and International legal regime, Available at: https://shodhganga.inflibnet.ac.in/bitstream/10603/250817/10/10_chapter-iv%20%20cybercrime%20issues%20and%20international%20legal%20regime.pdf
- Gautam, Ritu, Cyber crime in India, Availablr at: http://hdl.handle.net/10603/250817
- Paranjape, Vishwanath, Legal Dimensions of Cyber Crimes
- Preventive Laws with Special Reference to India, (Central Law Agency Publication, Allahabad, 2010).

6

DIGITALIZATION AND SOCIO-LEGAL CHALLENGES

KEYWORDS

DIGITALIZATION, CYBER FRAUD, CHILD PORNOGRAPHY, PROTECTION MECHANISM, CYBER SENSITIZATION

CHAPTER SIX

DIGITALIZATION AND SOCIO-LEGAL CHALLENGES

AUTHORS

DEEKSHA, PH. D SCHOLAR, SHARDA UNIVERSITY, GREATER NOIDA, UTTAR PRADESH, INDIA

DR. SUSHMA SINGH, ASSISTANT PROFESSOR, SHARDA UNIVERSITY, GREATER NOIDA, INDIA

ABSTRACT

Based on six major technologies the Internet of Things, robotics, biometrics, persuasion technology, virtual & augmented reality, and digital platforms we address the social and ethical challenges that digitization raises. Our research of the scientific literature on the dominating technologies reveals six repeating themes: privacy, autonomy, security, human dignity, justice, and. In this paper, we emphasize the numerous changes in the digitizing society that seem to be at contradiction with these themes. harmony of power.

This study demonstrates how the recent digitization surge is stressing these common values. Stakeholders must be fully aware of these challenges in order to properly build the digital society in a socially and morally responsible manner. The largest advancements in supervision have been made in the fields of data protection and privacy. Regarding other moral concerns raised by digitization, such as discrimination, autonomy, human dignity, and an unfair power structure, there is less organisation in the supervision.

INTRODUCTION

Digitization and information and communication technology (ICT) are pervasive in contemporary culture. Nanotechnology, biotechnology, and neurotechnology are just a few of the various technologies that are connected to ICT. Since the late 1990 this so-called NBIC convergence has been more and more obvious. Every part of our life has been infiltrated by technology, which resides within us (for instance, through brain implants) and between us (for example, through social media like Facebook). Technology also continuously learns about us through big data and techniques like emotion detection. Less like us (robots and software exhibit intelligent behavior and can mimic emotions). This is the "intimate technological revolution," according to Van Est. The societal transition to digitization pushes the limits of human capacities and creates a wealth of opportunities, but also tests the limits of human morality. On the basis of six prominent technologies—the Internet of Things, robotics, biometrics, persuasive technology, virtual & augmented reality, and digital platforms—we discuss what social and ethical challenges arise as society gets more digital in this article.[1]

Robotics and the Internet of Things (IoT) primarily affect our physical environment, including our homes, workplaces, and public spaces. IoT is built on a global network that blends the real and virtual worlds of a website. The development of IoT has put us on the on the cusp of a new era where people and things in the physical world can automatically communicate information and be tracked. Can automatically share information.

In this way, the alarm clock does more than just wake us up. It also turns on the coffee maker so we can have fresh coffee with our breakfast, notifies us when a product has expired in the fridge, or changes the lighting in the room to match the action taking place in the video game we are currently playing.

Many IT firms anticipate that IoT will permeate every aspect of our daily life in the future. The augmented reality glasses that use the Internet to provide users with additional information about their environment in real-time or a biometric camera that can be connected to an online database to recognise faces are just two examples of the many IoT technologies we discuss in this article. Robotics and IoT development are closely related. Robots, like IoT devices, are typically outfitted with sensors to read their environment. They are becoming more connected to the cloud to share and analyse data and to perform independent actions based on such assessments. Robotics consequently raises a unique set of ethical problems, even though some of them overlap.

The increased usage of ICT also implies that interactions between individuals and between individuals and organisations are being digitised through augmented and virtual reality and digital platforms. Therefore, digitalization permeates our social and cultural world: we do more and more of our purchasing, transactions, music listening, friend-contacting, taking action, and dating online.

Communication has changed significantly as a result of the rise of social media and other internet services in the late 1990s and the new century.[2]

[1] Nedyalkova, Plamena; Andreeva, Andriyana; Yolova, DIGITALIZATION AND THE NEW LEGAL AND ECO NOMIC CHALLENGES TO EMPLOYERS IN IMPLEMENTING INTERNAL CONTROL.(Economic Studies . 2021, Vol. 30 Issue 5, p158-175. 18p.), 2021

[2] *Ibid*

IoT allows for the interchange of an increasing amount of personal data about us without our knowledge or consent. The privacy statement that comes with your smart TV from Samsung informs you that the company logs where, when, how, and what time you turn on your TV. The TV also includes a microphone for speech recognition and a camera for face recognition. Please be aware that if your spoken words contain personal or other sensitive information, such information will be among the data gathered and communicated to a third party, according to a warning in the Samsung TV's handbook. taken and forwarded to a third party. This caused quite a stir. The illustration demonstrates how consent is unintentionally granted when consumers are unable to comprehend the entire manual or experience "consent fatigue" as a result of the numerous permissions they must obtain about the usage of data that devices acquire. This begs the question of who is ultimately responsible for this process should the user be expected to carefully review the terms of use for every single device? Or is there also some blame to be placed on these devices' manufacturers? They ought to guarantee a certain reasonable expectation of privacy, don't they?

We can actually be tracked everywhere thanks to IoT, which can result in a great deal of openness at the expense of our privacy. The majority of the time, the manufacturer, not the user, is the owner of the data collected by smart appliances like washing machines, thermostats, televisions, and toothbrushes. Because IoT devices may be used inside of our homes to monitor household functions, the home which we traditionally think of as our private domain becomes transparent. As the walls and drapes no longer shield the house from prying eyes, the line separating inside and outside is becoming more and more hazy. Koops and Prinsen make the case for safeguarding citizens from this digital eavesdropping and for granting them both physical and digital privacy in their homes. This should offer security from outside technical assistance-enhanced observation, allowing citizens to enjoy a space where they can be most authentically themselves.

Biometric technology has a double-edged sword in terms of privacy. It can be used to safeguard privacy by just requiring the bare minimum of data to decide if someone is allowed to do anything, like enter a building or purchase alcohol. On the other hand, since biometrics may recognise sensitive information, managing what happens to that information may be challenging, particularly now that the technology has advanced to the point where it can be used in a wide range of devices and circumstances. [3]

Digitization also brings about significant criminal issues, such as hacking or DDoS (Distributed Denial of Service) assaults that render websites or systems inoperable.

The Internet or devices connected to the Internet can potentially be the target of criminal activity. Experience has taught us that almost any digital system may be compromised. For instance, in 2012, University of Texas researchers showed the US Department of Homeland

Security how comparatively easy it was to hack into and take over control of a military computer system. They accomplished this via a method known as spoofing, which involves impersonating the person in possession of a device in order to gain unauthorised access to it. In fact, there is a concern about cyber terrorism in policy circles. terrorism online in government circles.

[3] *Ibid*

Sensitive information can also be accessed by hackers, and if it does, it might fall into the wrong hands. The precise times of day or week when we turn down the heat and are obviously not home could be known to robbers by using a smart metre that has been compromised. Criminals have the ability to take control of smart gadgets in addition to extracting information that is important to them. This gives the security issue a physical component. A security researcher showed how easy it is to hack the Cayla doll, making it quote lines from The Silence of the Lambs' fictitious psychopath Hannibal Lecter and the sexual novel Fifty Shades of Grey. The hacking of the doll is a pretty innocent example, but New Zealand hacker Barnaby Jack demonstrated how to hack his friend's insulin pump.

DIGITAL MEDIA TYPES

Since we are aware that the notion of digital media is too broad to be adequately defined in a brief definition, we may at least attempt to comprehend its range by being aware of its presence in many forms:

Videos: There are billions of videos already online, and billions more are being added to the internet every second. By virtue of videos, digital media develops into visual digital media. Digital media fully exploits the idea that something may be understood more easily in a visual for than in other form. For instance, YouTube and Netflix are two of the most well-known internet platforms in the video sector.[4]

Fun Facts: In the visual market, YouTube, which launched only a decade ago, has grown to such a size that more than 500 hours of videos are uploaded there every single minute and more than 5 billion videos are seen their daily. The process of trying to comprehend the scale and influence of digital media has just begun.

Audio: Due to the variety of ways that audio is made available through digital media, it is currently just as popular as videos. Now it's as simple as unlocking one's smartphone and playing their favourite music, as opposed to the past when one had to wait for someone to request a song they liked or for the radio jockey to play something appropriate for the mood. In India, audio platforms like Google Play, Apple Music, and Spotify are quite popular since they quickly meet the needs of music enthusiasts while also offering podcasts, radio services, audiobooks, and other services.

Endorsement: The same is true of advertisements in digital media. Digital media marketing is currently popular since it offers a variety of marketing possibilities and makes it easy to reach the target audience, or, let's call them potential customers. The skippable and unskippable ads, pop-ups, and banner ads are created for each platform in a way that strikes a delicate balance between the needs of the marketer and the needs of the user. Thanks to the development of digital media, browsing the classifieds in the yellow pages seems to be a thing of the past.

[4] R Sai Gayatri, All you need to know about digital media and the legal challenges involved in it, pleader intelligent source, (june 2 2021), https://blog.ipleaders.in/need-know-digital-media-legal-challenges-involved/

Social Media: Can you imagine not having access to social media today? Seems to be impossible, no? We have all become enmeshed in the web of social media, whether deliberately or unknowingly, for a variety of reasons. For instance, you can use Twitter to voice your opinion, Instagram to share photos, LinkedIn to make it simpler to get a job, Facebook to connect with friends, and so on. Every social media network promotes one of its own important goals in order to bring users to it. Why would you turn down the chance to keep in touch with the people you care about with just a few simple finger taps? A lot of these outlets have been made possible by digital media. Social media should, however, be utilised with prudence because, after all, a bee shouldn't drown in honey.[5]

Literature: It's been stated that some hobbies are difficult to give up, and reading is one of the most well-known pastimes in the world. By integrating technology and digital media, readers' requirements have been met through the creation of e-books, e-magazines, and other products. With the aid of digital media, there are many platforms made available for readers to access millions of books, periodicals, or magazines for free or with a subscription. The pupils have also found the e-books and VR to be beneficial because they offer a lot more information than the typical paperback books.

Legal Issue: Digital media is a dynamic and ever-evolving notion that incorporates many different circumstances where people, businesses, designers, and others are exposed to many hazards that frequently result in legal disputes. Tell us more about the difficulties and legal restrictions posed by digital media.

INTELLECTUAL PROPERTY

Intangible commodities are the subject of intellectual property. Symbols, designs, words, thoughts, and inventions all fall under this category. Because it has audio and video components that may be downloaded from the internet, it also deals with digital media. The following are a few examples of digital media-related intellectual property rights.

Trade Mark and Digital Media

Numerous corporations and businesses are developing trademarks for themselves in the online space as a result of the fierce rivalry in digital media. Because digital media is viewed as a consumer-rich platform, marketing companies strive to use the internet medium to connect with the right customer at the right moment. As crucial as it is to expand your business, it's also crucial to protect it, and one way to do that is by registering a trademark for it.

The trademark enhances brand recognition and goodwill in addition to providing company protection. Even if it is virtual, digital media marketing puts businesses closer to their customers, increasing both sales and profits. As a result, it is critical to be active on digital platforms to compete in the market. Therefore, if you want to safeguard the value of your brand and goodwill from unauthorised parties, you should have registered a trade-

[5] *Ibid*

mark for your company. The Trademarks Act of 1999 regulates trademark law in India.[6]

Copyright and Digital Media

According to the Copyright Act of 1957, which governs copyright law in India, producers of musical, dramatic, artistic, or literary works as well as those who make sound recordings or make movies have an exclusive right to preserve their work, known as copyrights. These rights may include the ability to translate the work of such a creator or producer and to adapt, reproduce, and communicate it to the public. When all of these rights are combined, they take the shape of copyrights, although the extent to which they will be applied depends on the inventor or producer's work.

In the world of digital media, there is a vast amount of content that may or may not be protected by the owner's copyright. The worrying aspect about this situation is that people continue to copy other people's work, whether or not it is protected by copyright. Such violators now have a channel through which to violate the copyrights of the real creators of the work thanks to digital media. An owner must establish that he is the legitimate owner of that specific work and the source of the liability in order to demonstrate that his copyrights have been violated.

Patents and Digital Media

An invention is granted a patent, which is an exclusive privilege. In technical terms, an invention like this usually refers to a tool or a process that makes a new way of accomplishing something or a fix for a problem possible. A patent offers its owner twenty years of protection. The Patents Act of 1970 governs patents in India. Digital patents are those that deal with computer-related inventions, particularly those that have to do with how software is used. Any person who violates a patent by using the exclusive rights of the holder without the holder's consent is guilty of patent infringement. Sections 104–114 of the Patents Act of 1970 deal with patent infringement.

Deformation and Digital Media

The internet offers many platforms via which one can freely express one's views and beliefs. Nevertheless, this media is also employed to disseminate falsehoods about another person that harm their reputation.

According to Section 499 of the Indian Penal Code, 1860, the act of a person who states or publishes any matter regarding any person with the intention of defaming that person or knowing or having reason to believe that such statement or publication will defame that person's reputation is said to constitute defamation

against that person.[7]

For a statement to be considered defamatory, it must be both false and harm someone's reputation. It is simple to invent and create false information on specific people thanks to the widespread and easy access of information on digital media, not to mention the vast creation of false accounts with the intention of spreading

[6] *Ibid*

[7] *Ibid*

defamatory claims. Consequently, it becomes significantly more challenging to find each of the offenders in this case. Even the media promotes such unfounded presumptions and ideas in order to achieve high TRPs, which does not harm the offenders but has a tremendous negative impact on the lives of the targeted individuals. Defamation is thus a crucial legal concern in relation to digital media.

According to Section 500 of the Indian Penal Code, 1860, defamation is punishable by a simple sentence of up to two years in prison, a fine, or both. Rajiv Dinesh Gadkari filed a lawsuit against Smt. Nilangi Rajiv Gadkari in the case Rajiv Dinesh Gadkari v. Smt. Nilangi Rajiv Gadkari after getting a divorce letter from him for constantly harassing and defaming her through offensive photos. Accordingly, the defamation offence has been recorded.

PRIVACY INVASION

One of the most valued aspects of the online world is privacy. Nobody wants their private affairs to be used as a source of mockery or judgement. There is a limit to how much of oneself they wish to reveal with others, and this limit is individual to each person. Nobody can be made to divulge information without their consent. We frequently see adverts for products relevant to the items we search for online. Cookies and IP addresses are responsible for this. Cookies are text files that keep track of and record information a user has viewed on his or her device, and an IP address reveals a user's location.

The majority of online marketers cleverly gather user data through cookies and IP addresses. Many digital media sites attempt to harvest user data without the user's consent for their own gain. A person's personal information—which they would prefer not to share—is taken without his or her agreement and used for business or other similar objectives. This is known as an invasion of privacy. In other instances, such data is also utilised to target a person and obtain illegal advantages.

Every person has the right to request privacy in specific situations. The right to privacy is a basic right, according to the Supreme Court of India, and is inextricably linked to Article 21 of the Indian Constitution. As a result, any invasion of privacy that results in a person can be contested in court. Digital media should not be used to violate people's privacy or unjustifiably compile data from databases.[8]

[8] *Ibid*

7

NEURO – BASED JURISPRUDENCE IN CYBER VERDICTS

KEYWORDS

NEURO - SCAN, NEURO - CELLULAR PRISM AND NEURO - MOLECULAR HELIX

CHAPTER SEVEN

NEURO – BASED JURISPRUDENCE IN CYBER VERDICTS

AUTHORS

COLONEL PROFESSOR DR J SATPATHY, VISITING PROFESSOR, SCHOOL OF LAW, XIM UNIVERSITY, BHUBANESWAR, INDIA

PROF ANITA SINGH, PROFESSOR, SCHOOL OF LAW, SHARDA UNIVERSITY, GREATER NOIDA, INDIA

ABSTRACT

Neuroscience does not offer life's questions as these are normative in character. What visions can behavioral knowledge offer cyber verdict makers and responses (interaction) with those they lead? What management graces, dispositions and comportments are efficacious and on which catalogs? What can we learn about reward mechanisms and organizational design vis-à-vis these findings? Judges deliver verdicts based on evidence, facts, figures, statements and audio -video proof as presented. It is a surviving body of practicalities or substantial demonstrating whether a certainty or scheme is true or binding. Evidence may be real evidence, demonstrative evidence, documentary evidence and testimonial evidence, to list a few. Evidence encompasses encumbrance of proof, acceptability, significance, weight and modicum of what should be acknowledged into the record of a lawful proceeding. Based on these are bedrocks of neuro - cyber jurisprudence verdicts. Question is; do these hold reasonable significance? Cross examination by defence counsel and prosecution counsel do provide some intelligent breakthrough. But can those be the two 'pillars of verdict'? What is the role of Honorable Judge in such a situation? Should Judges base his verdict based on evidences provided? Should he not apply his 'mind' to decipher the 'intention' before delivering his verdict? How about the truthfulness of statements rendered, witnesses produced and the like? Neuroscience is the emerging sciences with fast new horizons of research. Objective of this conceptual paper is to monitor philosophy of 'scanning' biology in jurisprudential behavioural models towards understanding neurobiological drivers (EEG, ECG, Fmri, Eye Tracking, Skin Conductance, fNIRS, TMT etc.) that underlie behaviour and legal verdict making by means of fundamental tools from, psychology, neuroscience and biology. Methodology presents neuro - apparatus investigations in verdict deliverance. This requires an assessment in multiple, conceptually incompatible dimensions. This includes hybrid modelling attempt with an empirical backdrop. Purpose is to assess that neuro - apparatus investigations have stimulus on 'Judges Choice' with reference to prediction, mind-reading, responsibility, treatment and enhancement. Taking a systems-level approach, focus is to replicate philosophy of 'scanning' biology in neuro - cyber jurisprudence verdict research. Effects demonstrate indications for extemporaneous counterfactual replication. Major finding is that neuro - cyber jurisprudence verdict research attempts to decide and evaluates prospective verdict using neuro - cyber jurisprudence medium. The achievements of neuroscience shall co-operate better formulation of law and judicial cyber verdicts for a fairer judicial system. Conceptual paper discusses new findings to understand neuro-cyber jurisprudence chromosomal design and offers to answer issues in data - driven leadership verdict-making dynamics.

> *For we all agree that the most excellent man should rule, i.e., the supreme by nature, and that the law rules and alone is authoritative; but the law is a kind of intelligence, i.e. a discourse based on intelligence. And again, what standard do we have, what criterion of good things that is more precise than the intelligent man? For all that this man will choose, if the choice is based on his knowledge, are good things and their contraries are bad. And since everybody chooses most of all what conforms to their own proper dispositions (a just man choosing to live justly, a man with bravery to live bravely, likewise a self-controlled man to live with self-control), it is clear that the intelligent man will choose most of all to be intelligent; for this is the function of that capacity. Hence it's evident that, according to the most authoritative preference, intelligence is supreme among goods.*

..... Aristotle (in '*Protrepticus*')

INTRODUCTION

Everyday life is full of cyber verdicts and choices. An important question for many researchers is how Judges make (mathematical modelling) cyber verdicts. Specifically, researchers are interested in assumptions, beliefs, habits, and tactics that Judges use to make every day cyber verdicts. Research suggests that cognitive architecture considers various sources of information before making a cyber verdict. However, how does it do this? In addition, why does the process sometimes go skewed, causing impulsive, indecisive, and confused cyber verdicts; that lead to risky and potentially dangerous behaviours? Human behaviour is not the product of a single process, but rather reflects interaction of different specialized subsystems. These systems usually interact seamlessly to determine behaviour, but at times, they compete. Result is that cognitive architecture sometimes argues with itself, as these distinct systems come to different conclusions about what we should do. Human behaviour is not under constant and detailed control of careful and accurate hedonic calculations. It is product of an unstable and irrational complex of reflex actions, impulses, instincts and habits.

Expansion of neurojudicial modelling parallels development of cognitive science. Neurojudicial mathematical modelling has bridged contrasting fields of mathematical modelling and psychology. Mathematical modelling, psychology, and neurojudicial science converge into a single, unified discipline with ultimate aim of providing single, general theory of human behaviour. This is the field in which consilience operates. Researchers and psychologists provide conceptual tools for understanding and modelling behaviour. Neurojudicial researchers provide tools for the study of mechanism. The goal is to understand processes that connect sensation and action by revealing neurojudicial mechanisms by which cyber verdicts are made. Neurojudicial findings have posed challenge to standard mathematical modelling perspective. The important source of inspiration has been neurojudicial judgment research (amalgamation of ideas from cognitive science and mathematical modelling). Neurojudicial mathematical modelling has primarily challenged customary mathematical modelling postulation that cyber verdict - making is a unitary process, suggesting instead that it is driven by interaction between automatic and controlled processes. Despite substantial advances, question of how we design and craft judgments and cyber verdicts has engaged researchers for decades. Different disciplines approach the problem through characteristically different techniques. Neurojudicial cyber verdict making has emerged as an inter-disciplinary effort to bridge this gap. It integrates ideas from fields of organisational psychology, neurojudicial science and neurojudicial - mathematical modelling to specify accurate models of cyber verdict making. Research investigates neural bases of cyber verdict predictability and value, central parameters in expected utility to cyber verdict – making. Integration of these offers exciting potential for construction of near - accurate models of cyber verdict - making.

In general, study of cyber verdict has been partitioned into three main approaches. For most researchers, goal of studying judicial cyber verdict behaviour is prediction. These scientists seek to develop formal mathematical models, typically based on rigorous axiomatic foundation, which can predict judicial cyber verdicts, or should, make. These models typically take as inputs state of external world and generate as outputs actual cyber verdicts made by judicial choosers. For a mainstream researcher, a model is useful if it makes accurate predictions; whether or not the algorithm it employs mimics the actual process of cyber verdict - making is irrelevant to accomplishing this end. For this reason, mathematical modelling studies of cyber verdict - making can be viewed as aimed towards achieving both; compact and abstract models of cyber verdict possible. The yield is high-level, and often normative, theories that state testable neurojudicial hypotheses.

PHILOSOPHICAL PERSPECTIVES

Aristotle, who was of the firm judgement that Anthropoids have a rational soul that can experience sensations and thoughts with the innate capacity to absorb forms of varied objects and to relate them using the brain and logic, and present a compounded amalgamation of the several suppositions collated with logic and observation to make general, causal claims. He studied that the derivable rationality of any conflict can be determined by its architecture rather than its internal components. He believed that the study of the environment would be the major type of comprehension, if there were no other individualistic objects apart from the blended and complex innate ones. However, if there is any inanimate individualistic object, the understanding of the same dominates and is the initial credo to guide a person. It automatically becomes ubiquitous as it is initial. Moreover, it is a kind of understanding which comprehends a vital force as a vital force, a life as a life; just by virtue of its existence.

Aristotle believed the chain of thought, which ends in recollection of certain notions and judgements, was associated methodically in relationships such as similarity, disparity and propinquity. The first imperative was not to deliberate in a state of hurry. Second imperative was to verify all information. Third imperative was to consult and listen. Fourth imperative was to consult or at least look at the situation from the perspective of all parties who will be affected. Fifth imperative was to examine all known precedents. Sixth imperative was to calibrate the likelihood of different outcomes. Final imperative was to apply just preferences by weighing evidence and deliberating each case individually. Don't multiply entities beyond necessity. One should handpick a solution with least suppositions. This was propounded by Occam (1287 - 1347). He opined that if there are two elucidations and conclusions that make the same prognosis, the one which is backed by the lowest number of suppositions which have no corroboration, is preferred, until more evidence and authentication comes along. First mandate was that the naivest elucidation is practically constantly par aggregate. Second mandate was ceteris paribus, one ought to choose a path that develops from scarcer guesses or suppositions (*'Entia non suntmultiplicandapraeter necessitate'*). Third mandate as to explicate singularities by unassuming postulate conceivable. Swinburne (1997) is of the belief that the easiest conjecture propounded as an elucidation of situations is more likely to be the authentic and fact-based one, than in any other available conjecture. Also, that its forecasts are more likely to be true than those of any other available postulation. Also, that it is an ultimate *deduced and self-evident* hemato - cerebral principle that lucidity is an attestation for truthfulness. Influential in replacement of Aristotelian viewpoint, Francis Bacon was of the view that the most intense delusions inherent in the thinking process of Anthropoid beings are impacted and influenced by unscrupulous predilections, which tend to negatively affect the prolepsis and comprehensive power of the Anthropoid brain. Francis advocated for prospect of logical understanding grounded upon inductive hemato - cerebral and cautious reflection of measures. Individual has predilections surrounded by choice substitutions that permit to state which alternative they choose.

> *'If we ought to philosophize we ought to philosophize, and if we ought not to philosophize we ought to philosophize; in either case, therefore, we ought to philosophize. If rationale exists we ought certainly to philosophize, because rationale exists; and if it does not exist, even so we ought to examine why it does not exist, and in examining this we shall be philosophizing, because examination is what makes rationale'*
>
> ...... *(Aristotle).*

Judicial performance has been subject of active research from several perspectives. Neurojudicial mathematical modelling explains judicial cyber verdict-making, ability to process multiple alternatives and choose an optimal course of action. It studies how mathematical modelling behaviour shape understanding of cognitive architecture and guide models of mathematical modelling via. Neurojudicial science, neurojudicial mathematical modelling, cognitive and organisational psychology. As research in cyber verdict - making behaviour becomes computational, it incorporates approaches from theoretical biology, computer science and mathematics. Neurojudicial mathematical modelling adds by using methods in behaviour and neural mechanisms. By using tools from various fields, Neurojudicial mathematical modelling offers an integrative way of understanding cyber verdict making. If further proof were needed, neurojudicial mathematical modelling provides evidence to explain cyber verdict-making, ability to process multiple alternatives and choose optimal course of action. It studies how mathematical modelling behaviour shape understanding of cognitive architecture and guide models of neurojudicial.

Deciphering cognitive architecture - environment transactions require mechanistic understandings of neurojudicial processes that implement value-dependent cyber verdict-making. There is a crucial difference between ‘thinking about thinking’ and actually enhancing cognitive architecture and mental processes by developing latent potential of each Judge. Theoretical accounts posit that judicial cognitive architecture accomplishes this through series of neural computations, in which expected future reward of different cyber verdict options are compared with one another and option with highest expected value is selected. If judicial cognitive architecture is often compared with a computer, goals for biological cognitive architectures are determined by need for survival in uncertain and competitive environments. How to handle cognitive architectures behind judgments in age of dramatic change and growing uncertainty? What then are the coherent cognitive architecture dynamics underlying prediction, control and cyber verdict-making?

Quantification of cyber verdict has been a major area of research for neurojudicial scientists. This is, in part, due to the ‘Matching Law’ that stipulates that relative response rate on concurrently available alternatives ‘match’ available relative reinforcement rates. This theoretical construct describes response allocation in complex situations. Judges often attempt to design ‘rational’ cyber verdicts. Mathematical modelling agents are subject to multiple biases that affect events, act upon them and learn from experience. These behaviours have disastrous consequences. When faced with complex cyber verdict, Judges engage in simplifying strategies. Adaptive cyber verdict making relies on strategic simplifications of cyber verdict problems. Yet, neural mechanisms that shape these remain largely unknown. Although cognitive architecture encodes specific cyber verdict factors, much less is known about how cognitive architecture selects among multiple strategies for managing computational demands of complex cyber verdict - making task. Advances in cognitive architecture connectivity have made it possible to identify hubs; cognitive architecture’s connected regions. Such regions coordinate cognitive architecture functions due to their connectivity with regions with variety of specializations. Current structural and functional connectivity methods generally agree that default mode network (DMN) regions have highest comprehensive cognitive architecture connectivity. Control of behaviour is fundamental to judicial cyber verdict making. Evidence suggests a front parietal cognitive architecture network implements such control across diverse contexts. Lateral prefrontal cortex (LPFC) region predict performance in high control task and exhibit high connectivity. Critically, connectivity in this region shows highly selective relationship with Judge differences in fluid cyber verdict making. LPFC facilitates ability to implement control processes central to judicial cyber verdict making. The ability to rapidly reconfigure minds to perform tasks is important for adapting to an ever-changing world. Further, it is unclear how this kind of task preparation changes. Research suggests that prefrontal cortex is essential to perform tasks.

Neurojudicial cyber verdict - making is as a mental process (cognitive process) resulting in selection of a course of action among alternative scenarios. Every cyber verdict - making process produces a final cyber verdict. Process must be regarded as a continuous process integrated with environment concerned with logic of cyber verdict making, rationality and invariant cyber verdict making. This reflects interaction of cyber verdict making-related regions. Specific cognitive architecture systems potentiate cyber verdict makings depending on strategies, traits and context. Therefore, cyber verdict making is a reasoning or emotional process which can be rational or irrational, based on explicit assumptions or tacit assumptions. This exhibits formulation of '*neurojudicial cyber verdict making paradox*'.

CEREBRAL GUESTIMATES

Quantification and qualitative exposition of choosing an alternative is, in part, on account of 'Matching Law' (connection that holds between comparative rates of response and comparative rates of underpinning in simultaneous agendas of underpinning). Amalgamation between behavioural and neural science with managerial economics, neural mechanisms reveal about how cerebrum encodes specific preference factors. Are we imminent on the management preference issues and corresponding preferences with the veracious perspective? This issue has persistently cropped up leading to managerial preference intricacies perfectly perched on managers' choice behavior. Theoretical exponents' developed architectures that calibrated pre -disposition of relatively multifarious preference making mechanisms. This is paving way for lab setting architectures in Cerebrum Plotting and charting (Eye Tracking, *Skin Conductance* / EDA, *MRI,* MRI, *BOLD, EEG,* MEG, *ECG,* TMS, CT, PET, SNM, BOLD and DCS*)*. Chromosomal micro feasibilities of preference crafting has conservatively acknowledged significant consideration from Loewenstein (2001), Slovic (2002), Tversky and Kahneman (1975), Bechara (2004),Clark (2003), Damasio (1996), Lhermitte (1986), Shallice and Burgess (1991), Ernst (2004), Paulus (2003),Rogers (1999), Clark (2004), Glimcher (2002), Gold and Shadlen (2001), Platt and Glimcher (1999). Maidenin roads were initiated from Bechara (2004) and Damasio (1996). These exceptional arrivals registered cerebrum expanses obligatory for adaptive judgement crafting and provisioned abstract depictions of critical planes of preference carving (Damasio; 1996). Perennial and corroborative incursionary incursion of facts, figures, statistics or data has inundated the preference maker with drifts, inclinations and trends and patterns or template of behaviour that impetuses to reconnoiter prospects to alter and overhaul philosophies to suit current 'preference' needs. The imperious issue is whether there is a prerequisite to review prevailing 'theoretic models'? If in the affirmative, will that come about with toting to standing frame of information or obliterating more or less some vital central mechanisms? Do 'preference' management transcripts necessitate interdisciplinary schemes to explain 'preference' in a better connotative framework? What then would be the general insinuations of cognito (managerial) management? Attention is on '*Bereitschaftsprobable'* (German) meaning ‘pre-motor probable’ or ‘gameness prospective’.

CONCLUSION

Goal of studying judicial cyber verdict behaviour is prediction. This research seeks to develop theoretical models, based on axiomatic foundation, which can predict judicial cyber verdicts. These models would take as inputs state of external world and generate as outputs actual cyber verdicts made by judicial choosers. For this reason, research would aim towards achieving compact and abstract models of cyber verdict. To date, cognito modelling model of cyber verdict has not been informed by the way cognitive architecture functions. Analysis of observations would include not only choices between options, per se, but additional data, including length of time taken to make cyber verdicts, number of errors in cyber verdicts and psychophysical model(s).

Including more than just observed cyber verdicts allows data to have an additional disciplining effect on theory. We extend this assumption of optimal behaviour to analysis of cognitive architecture process producing a cyber verdict. To do this, we assume that there is an unobservable cyber verdict that an agent makes, consequences of which are reflected in all observable data that can be measured in the cyber verdict process. That cyber verdict is strength of effort devoted to processing information in reaching a cyber verdict between options. As a conclusion, we propose a model that joins predictions of traditional psychological observations and predictions of relative cognitive architecture activation dependent on exogenous characteristics of cyber verdict environment.

Even as it is recognised that cognitive architecture (and consequent behaviour) does not operate perfectly optimally, there are several reasons why these assumptions can nevertheless be valuable. First, although complex forms of behaviour might not be optimal, simpler evolutionarily conserved mechanisms might prove to be closer to optimal, or at least to have been so in the environment in which they evolved. Second, an assumption of optimality can be a crucial step in development of formal model. Formal model, in turn, enables generation of precise, testable predictions about Judicial behaviour. Finally, even when behaviour (or neural function) turns suboptimal, defining optimal performance can provide a useful benchmark against which to compare actual behaviour. Identifying ways in which behaviour systematically deviates from optimality can generate new insights into underlying mechanisms.

Neurojudicial cognito modelling model will play a crucial role in building of new reliable theories capable of explaining and predicting individual behaviour and strategic cyber verdicts. Main message is that individual is not one coherent body. Cognitive architecture is a multi-system entity and therefore cyber verdict-maker must be modelled as an organisation. Before the modern model, organisations were modelled as individual players characterised by an input-output production function. Systematic study of interactions between agents and cyber verdict processes within organisations lead to novel insights. Applying similar methodology to study Judicial cyber verdict - making is the way to understand bounds of rationality.

Neurojudicial cognito modelling offers solution through series of measurements of cognitive architecture activity at the time of cyber verdicts. It provides conceptual and philosophical framework for understanding and conducting research at intersection of neurojudicial science, cognito modelling and psychology. *Neurojudicial cognito modelling theory* proposes to build cognitive architecture-based models capable of predicting observed behaviour. Neurojudicial cognito modelling will shed light on causes of behaviour (and neurojudicial anomalies) and help build theories capable of explaining and predicting cyber verdicts. Measurement of cognitive architecture activity provides information about underlying mechanisms cognitive architecture during cyber verdict processes. Neurojudicial cyber verdict modelling would help when new information is inconsistent with goals. Combining the above disciplines gives interdisciplinary insight to define fundamentals of neurojudicial cyber verdict making that has eluded researchers.

REFERENCES

1. *Satpathy, J., Gankar, S. and Patnaik, J. (2020). Neuro - Couplings in Managerial Choice Preference, IUJ Journal of Management (IUJJOM), ISSN: 2347 - 5080, EOI: 10.11224 / IUJ, Volume 8, Issue. 1, Pp: 79 - 91, June, ICFAI University Jharkhand, India (National).*
2. *Satpathy, J., Wadhwa, C., Rodriguez, C. M., Hejmadi, A. and Laza, S. (2020). Neuro - Curvatures in Conscience - based business Cyber verdicts, Proceedings of International Conference on Conscience - based business, Information Technology and Enterprise Architecture, ICBIT - 2020, 25 - 26 September 2020, Management Development Institute ,Murshidabad, India (International). FORTHCOMING*
3. *Satpathy, J., Das, A. and Panda, M. and Gankar, S. (2020). Neuro - Cursors in Entrepreneurial 'Choice Mosaic', Journal of Juni Khyat, UGC - CARE Group I Journal, ISSN: 2278 - 4632, Volume 10, Issue 5 (14), Pp: 383 - 391, India (National).*
4. *Satpathy, J., Das, A., Laza, S. and Hejmadi, A. (2020). Experiment in Neuroentrepreneurial 'Preference', Journal of Juni Khyat, UGC - CARE Group I Journal, ISSN: 2278 - 4632, Volume 10, Issue 5 (6), Pp: 86 - 99, India (National).*
5. *Satpathy, J., Mallik, B. and Garg, S., Hejmadi, A. and Gankar, S. (2020). Skin Conductance in 'Smart' Managerial Judgement, Journal of Test Engineering and Management, ISSN: 0193 - 4120, Volume 83, Pp: 17581 - 17588, Mar - Apr 2020, The Mattingley Publishing Co., Inc., California, (USA) (International).*
6. *Satpathy, J. and Mallik, B. (2018). Hematological Judgement in Entrepreneurial Cyber verdict, International Journal of Management, Technology and Engineering, ISSN No: 2249-7455, Volume 8, Issue XII, Pp: 2849 - 2863, December, India (International).*

8

CYBER CRIME IN INDIA WITH SPECIAL REFERENCE TO WOMEN, CHILDREN AND SENIOR CITIZENS

KEYWORDS

PSYCHOLOGICAL FACTORS, CYBER FRAUD, CHILD PORNOGRAPHY, PROTECTION MECHANISM, CYBER SENSITIZATION

CHAPTER EIGHT

CYBER CRIME IN INDIA WITH SPECIAL REFERENCE TO WOMEN, CHILDREN AND SENIOR CITIZENS

AUTHORS

JOHN T LALDINGLIANA, LLM STUDENT, SCHOOL OF LAW, SHARDA UNIVERSITY

DR SANSKRITI MISHRA, ASSISTANT PROFESSOR, SCHOOL OF LAW, SHARDA UNIVERSITY, GREATER NOIDA, UTTAR PRADESH, INDIA

DR. RITU GAUTAM, ASSISTANT PROFESSOR, SCHOOL OF LAW, SHARDA UNIVERSITY, INDIA

ABSTRACT

With the increasing use of computers in society, cybercrime has become a major issue. And now cybercrime is one of the most complicated issues of the cyber world. “Cybercrime is basically an illegal act in which a computer is either a tool/ mean or target”. The evolution of the internet provides easy access to data and information from anywhere over the globe. Any person can access the

information over internet from their any place in the world. However, there are some drawbacks also. Instead of being benefitted with the facilities of internet, some peoples tend to misuse the computers and internet for crime. There are different categories of have taken birth over internet as cyber pornography, cyber defamation, cyber bullying, cyber grooming, cyber stalking, email bombing, carding, cheating and fraud, virus attacks, web jacking, hacking etc. In this article, the author analyzed the easier access to internet and social media resulting in increasing cyber-crimes against women, children, and senior citizens in Indian society. There are several crimes known and unknown to normal person through which mostly women get victimized in way of Cyber staking, Harassment through e-mails, cyber-sex, Cyber defamation etc. and other than these crimes, crime minds use the cyber world's tools for child abuse which is also serious as it impacts the innocent minds of children. The crimes against the children using computer and internet are having different facets as exposure to sensitive content, possession, production and distribution of child pornography, cyber harassment, and sexual abuse, cyber bullying etc. Along with women and children, there is one more descendant who is easy target to cyber-attackers. Within the last decade, the number of senior citizens has been increased significantly among the internet users. It has been recorded in the past decade that senior citizen had the greatest rate of increase in Internet usages among all other age groups. However, senior citizens are prone to be targeted and exploited by cyber criminals specifically for financial crimes.

In this paper, the researcher discussed the various categories of cybercrimes which are commonly imposed upon a woman, children and senior citizens, further the researcher analysed that how these crimes adversely affect them. The researcher also briefly examined the various laws for the protection of women, children and senior citizens; (i) Information Technology Act (2000), (ii) Constitutional liability, (iii) The Protection of Children from Sexual Offences (POCSO) Act, 2012, (iv) The Indian Penal Code (IPC), 1860

Lastly, the author focuses on the remedies available to the victims of cybercrime and the changes required in the legal system to effectively curb the rising spirits of cyber criminals.

INTRODUCTION

The invention of Computer has made the lives easier as it was never before; it has been using for various purposes starting from the individual to large organisations across the globe. Nowadays Internet is becoming part and parcel of a modern lifestyle of the people throughout the world. It is simultaneously empowering, fascinating, difficult, and dreadful. To most of the people, the Internet remains mysterious, forbidding, incomprehensible and frightening. Since decades, the majority of computer users have been misusing the technology, either for their own profit or that of others. This gave birth to "Cyber Crime".

Every year on March 8, we celebrate International Women's Day to show our respect, love, admiration, and gratitude for women. Even in our traditional ancient Indian society, women were placed at a very high position, The Vedas revered women as a 'Devi' and praised them as the mother, the creator, and the one who gave birth. But now the situation is not so well. India being one of the worst countries in the world for the exploitation of women. Women and children are among the most vulnerable members of society, making them easy targets for cybercriminals. This was especially true during the epidemic, even though men and adults were also susceptible to numerous cybercrimes. For many decades and indeed today, women have been harassed in numerous ways. Domestic violence, Sati Pratha, acid-attack, rape, eve-teasing, sexual harassment, dowry death, molestation, kidnapping, honor-killing, female infanticide etc. are some forms which come into the category of violence against women. In modern time women are viewed and portrayed as sex objects, she is inferior to men in our society, this has created a huge gender bias between the men and women where the has typical mentality that their wrongdoings towards women cannot be penalized. This gift of the internet is used by the criminally inclined to commit wrongdoing and then conceal themselves under the cover given by the internet. The cyber world in itself has a virtual reality where anyone may conceal or even fabricate his identity.

Everyone over the world has had a rough time during the pandemic. The COVID-19 virus has been shown to be a catastrophe that has killed many people and caused millions of others to suffer mentally, physically, and emotionally. Millions of individuals have lost their lives as a result of the pandemic. The most susceptible and straightforward targets of these cybercrimes have been children, especially those who have either been abandoned because they have lost both of their parents or who have been temporarily separated from them because one of them has contracted an illness. In today's society children are the most endangered section and as a result of their lack of majority level, they are readily exploited in the cyber world. Nowadays, it is observed that even child sexual exploitation has started online. Cyber Crime is growing day by day and a large group of individuals became victims of hacking, theft, cyber stalking, fraud, malicious software, child soliciting etc. 'There are two main forms of this behaviour. The first involves using the Internet to traffic and/or collect child pornography. The second involves the widely publicized problem Children of adult men soliciting sex from minors on-line'. When children are separated from their parents or have no one to care for them, they are more vulnerable. Children are readily tricked into engaging in immoral behaviour and making themselves easy prey for cybercriminals since they lack the knowledge necessary to determine whether a specific website is acceptable to visit or not, as well as whether a particular image or video should be downloaded or not. Because of this, it's quite simple for sexual predators and other cybercriminals to access these kids' gadgets and manipulate them.

Cybercrime is on the rise as more people across the world use the internet. Estimates for the amount of money people and businesses have lost as a result of online fraud range from 100 billion. Over the world, the number of adults over 60 has increased rapidly in last decades specifically during covid pandemic. Older adults are a fast-growing group of internet users. Like the rest of the population, the growing adoption of internet technology has exposed older adults to threats of online crime. Although fraud affects people of all ages, older adults are disproportionately vulnerable. Older people were found to be attractive targets to criminals due to their perceived relative lack of familiarity with technology, relative wealth and hesitancy to report the crime to authorities due to feelings of shame.

LITERATURE REVIEW

1. **"Cybercrime against women and children", Aditi Shrivastava, 2021**

In this article the author provided that with increasing the rate of internet uses, the rate of cybercrime increased incredibly during the lockdown in India. A total of 704 cyber-crimes registered against women in 2020 and 504 in 2021 (till July). Cyberstalking, Sextortion, Cyber-Hacking, Cyber-Bullying, Sexual Abuse (including the use of pornographic and sexually explicit material against the victim), Cybersex Trafficking, and Phishing are the most frequent cybercrimes performed against women during the pandemic. Cyberbullying, child grooming, cybersex trafficking, and sexual abuse of minors are among the most prevalent cybercrimes performed against children during the pandemic. Due to their vulnerability, women and children were particularly easy prey for cybercriminals and sexual predators during the lockdown.

2. **"Cyber Crime and the Victimization of Women: Laws, Rights and Regulations", Debarati Halder, 2011**

   Cyber Crime and the Victimization of Women: A distinctive and significant addition to the literature examining several facets of cybercrime is Laws, Rights and Regulations. This book deals directly with a topic that is typically only mentioned incidentally, i.e. as a side effect of a particular cybercrime instance or concern. It investigates the gendered aspects of online crimes such cyberbullying, cyberstalking, defamation, modified pornographic photos, and electronic blackmail. Perpetrators who, for a variety of reasons, are unlikely to be identified or punished routinely use these and other methods to intimidate, control, and cause other harms. Researchers, academics, legislators, everyday women, and those who support them will learn more about cybervictimization and how to better respond to cybercrimes against women.

3. **"Everything about cybercrimes against women", A. Thiruthi, 2021**

   In this article the author summarises, while a crime-free society is impossible to achieve and only exists in fantasy, it should be a continuing effort to enforce regulations that reduce criminality to a minimum. Particularly in an increasingly technologically reliant world, criminality related to electronic law-breaking is certain to increase, and legislators must go the extra mile to keep impostors at bay. Technology is often a double-edged sword that can be employed for either good or evil purposes. To combat cybercrime against women, the Legal system has enacted a number of legislations. Thus, it should be the relentless efforts of rulers and legislators to assure that technology advances in a healthier way and is employed for legal and ethical economic growth rather than criminal activity.

4. **"Internet crimes against children", Keith F Durkin, 2012**

   Internet crimes against children are a contemporary social problem which has drawn a great deal of attention from the parents, educators, legislators, and law enforcement officials. This phenomenon has captured national attention in the United States with a number of media reports of this phenomenon. These crimes include child pornography offenses, as well as adults soliciting minors for sexual purposes on line. Drawing upon data from recent national surveys, the characteristics of offences, offenders, and victims are examined. A multitude of issues related to the assessment and classification of the individuals who commit Internet crimes against children are also explored. Strategies for the prevention of this behaviour and enforcement of laws protecting children online are discussed.

5. **"Older people's experience of cybercrime victimisation in Mumbai", Kartikeya Tripathi, 2019**

   In this brief report, the author described possible vulnerability factors for cybercrime among older people in Mumbai, as well as the potential impact of this crime. Report draws on the limited, existing literature on cybercrime and older people in LMIC and uses qualitative interviews with older people who have been victims of cybercrime in Mumbai and their supporters to illustrate and add to these findings. The sample size was small but suitably diverse for the first exploratory study of this nature. It was difficult for the researchers to recruit participants without convenience sampling in near total absence of official data on the subject. However, the final sample included victims of three most common types of cybercrime in Mumbai and their relatives. The experts interviewed represented the views of the major institutions—police, the legal system, investigators and Non-governmental organisations—who interact with older people who are victims of cybercrime. The perspectives author present highlights the importance of data protection in preventing online fraud, the need to provide older people, who constitute a high risk group, with the skills, awareness and tools to take precautions in sharing their private information and training of frontline staff in banks, phone companies and police stations on how to avoid data leaks and support victims when crimes occur. These preliminary findings can inform larger studies to support the design of safeguards for older, internet users in LMIC; as well as training for staff of banks and police on how to respond to older people reporting cybercrime.

6. **P. K. Vanita, (2012)**, has concentrated on the various issues related to the first-level and second-level technical knowledge of cybercrimes for detection, prevention, and investigation of cybercrimes against women. These issues relate to the prevention, investigation, prosecution, and punishment of cybercrimes by Indian law enforcement authorities.

7. **Virendra Kumar, (2018)**, has discussed the different types of cybercrimes committed against women. Author has pointed out that, increase in the users of Internet, there is an increase in cybercrime rate. Author has opined that victimised women should come forward and report against the crime in a special Anti-cyber crime cell. In the opinion of the author, awareness among women about cybercrimes, and usage of the Internet, social media will definitely help to curb the cybercrime, and there will be reduction in the cybercrimes.

8. **N. Agarwal, (2014)**, has discussed cyber crimes and outlined security vulnerabilities against women in India. Through the study the author has also understood the opinions/ perceptions of police officials, counsellor's cyber cell officials etc. about the cyber-crimes against women. Author has also discussed the Information Technology Act 2000.

UNDERSTANDING CYBER CRIME

Cybercrime is the term commonly used for illegal activities which can be done by using a computer and internet as its primary tools for commission. It is an offence when someone or a group of people uses contemporary telecommunication networks like the Internet to purposefully damage the victim's reputation or cause the victim's physical or mental harm either directly or indirectly. Women, children, and older citizens who are unfamiliar with the online world and have just recently begun using it are particularly vulnerable to falling for the traps set by online bullies and fraudsters. The following are the most common sorts of cybercrimes and cyberbullying that are committed online:

CYBER-CRIME AGAINST WOMEN

Women are considered soft target to be manipulated. Also lack of knowledge about the complexities of internet world, less exposure, lack of awareness are some key points which makes them prone to be target by criminal minds. Here are some categories of cybercrimes against women as;

- **Cyberstalking**

  It included connecting or trying to connect with the victim on social media or phone calls despite clear indication of disinterest from her end, posting messages (sometimes threatening) on the profile of the victim, constantly bombarding the victim with emails/text messages/phone calls, etc.

- **Sextortion**

  This is the most common cybercrime committed against women during the period of the pandemic. The offenders started extorting money or sexual favors by blackmailing the victims to reveal their private pictures or morphed images. The pandemic and lockdown frustration made the offenders seek sexual video calls/images or messages from women by threatening them. Also, loss of income encouraged them to extort money by threatening the victim with their morphed images.

- **Cyber hacking**

  During the lockdown, people started to read news online. There was a rise in cases of fake news and information. The women started becoming the victim of cyber hacking by clicking on malware links which get all their information available on phone, turns on the camera and microphone, and captures their intimate pictures and videos. Offenders, in turn, use these pieces of information and pictures for sextortion and other favors.

- **Cyberbullying**

  This included publishing defamatory and abusive statements against the victim on social media platforms and demanding money for deleting them, insensitive comments on the posts of the victim, exchanging morphed images/private images of the victim without her consent, sending rape threats to the victim, etc.

- **Phishing**

  To make money in lockdown, offenders are sending fake emails with a link to a particular webpage to induce the victim to unwittingly enter personal data like bank account details, contact details, and passwords or with the intention to install harmful viruses in the victim's device as soon as they open the link. These emails and messages appear to have come from legitimate sources. The offenders then make fraudulent transactions from the victim's account to their account with the use of the bank account and other personal details of the victim.

- **Sexually abusive and pornographic content**

During the pandemic, offenders were also indulged in sexual abuse of women on the internet, morphing the picture of the victim and using it for the purpose of pornography.

- **Cybersex trafficking**

Unlike sex trafficking, the victim does not come in direct contact with the abuser. In cybersex trafficking, the dealer live-streams, films, or photos of the victim performing sexual/intimate acts from a central location and sells the material online to sexual predators and buyers. The offenders have been sexually abusing women by making them a part of cybersex trafficking byways of coercion, manipulation, and blackmailing.

CYBER-CRIME AGAINST CHILDREN

Children and teenagers are next soft target to get in box easily. Here are some common forms of cyber-crimes against children which are described, they are;

- **Sexual abuse of children**

This includes child sexual abuse materials such as child pornographic images and videos, online sexual exploitation of children over phone call/video call where children are coerced into performing sexual acts.

- **Pornographic/sexually explicit content for children**

While using the internet for education and entertainment purposes or going through a social media page, children are being induced to open certain websites which direct them to sexually explicit content and pornographic videos/images. This corrupts the mentality of the child but the offender gets views and money.

- **Cybersex trafficking**

Unlike sex trafficking, the victim does not come in direct contact with the abuser. In cybersex trafficking, the dealer live-streams, films, or photos of the victim performing sexual/intimate acts from a central location and sells the material online to sexual predators and buyers. The offenders have been sexually abusing children by making them a part of cybersex trafficking byways of manipulation and coercion.

- **Cyberbullying**

This includes harsh, mean, abusive, or cruel comments and messages against the child victim. Children are easy to bully because of their innocent nature and it becomes even much easier for the offenders to bully children on virtual platforms. Cyberbullying causes; avoiding school classes via virtual platforms, suddenly wanting to stop using the internet and computer devices, being secretive about their digital life, distress, and emotional instability among children.

- **Child grooming**

The offender befriends the child victim by forming an emotional and fiduciary bond with him/her with the objective of sexual abuse of the child. The children tend to trust easily and hence, it becomes very much easy for the offenders to create such a bond with them. Once the bond is created, the offender starts manipulating the child to perform sexual acts. Child grooming via online platforms and social media has been one of the most committed cybercrimes during the pandemic. Child groomers were able to operate and gain children's trust online and it became easy for them to do so because of the unawareness of children and parents about the dark side of the internet world.

CYBER-CRIME AGAINST SENIOR CITIZENS

Due to age factor the learning and memorizing capability becomes lesser. And it became a good opportunity to cybercriminals. Some of the tactics of cyber criminals which they used to trap senior citizens are like;

- Deliberately spreading fraudulent reverse mortgage and loan offers.
- Pressuring elderly to pay in full or in part up front for services rendered by unregistered contractors. These thieves frequently never start or complete the work, costing the victims more money.
- Coercing senior citizens to provide their financial or personally identifying information (PII) in order to open new accounts.
- Pretending that family members creating credit cards in the victims' names or stealing money from their accounts.
- Charging fraudulent or unnecessary services using elderly victims' Medicaid or Medicare information.
- Targeting seniors with get-rich-quick pyramid schemes, or telling victims they've won a contest or the lottery. To collect, all they need to do is transfer a "small" amount of money to an account and then their winnings will be transferred to them.
- Influencing elders to make erroneous purchases, such as a coffin for a departed spouse when they will be cremated, by misleading them into doing so

These are just a few examples – the list goes on and on. While there are many other types of senior fraud, here are a few of the most common:

GENERAL STRATEGIES OF CYBER-CRIME FOLLOWED BY CYBER-CRIMINALS

Strategy 1: Online and Telephonic Phishing Scams

Everyone loves a good deal and women, seniors and children are natural soft target for that. Therefore, they are at top of the list of cyber attackers. They used to get frequently phone calls and emails with hidden scams or hidden cyber viruses. Free gifts vouchers, prizes, reward points, low-cost medications, low-cost goods and services and other items that seems good to be true (because they are). The criminals use these items and other interests as bait in a type of attack known as phishing.

Phishing typically refers to schemes that fool victims into supplying a range of personally identifying information (PII), bank account information, and login information through the use of unsolicited mails. Tactics often include the use of social engineering and language that evokes an emotional reaction such as fear or curiosity. Phishing can occur via email, over the phone (voice phishing, or "vishing"), and via SMS (SMS phishing, or "smishing").

Strategy 2: Identity Theft

People of all ages, colours, and socioeconomic backgrounds are victims of identity theft. It also takes many different forms, such as Social Security theft, tax refund theft, and medical identity theft. Online, over the phone, or by just obtaining the victim's information, identity theft can take place.

Strategy 3: Confidential Fraud

For many children and seniors, the internet represents a less intimidating way to connect with and meet new people. But this is also the playground of cybercriminals. These malicious actors use online platforms and other methods to conduct highly targeted attacks.

An elderly victim in this crime is tricked into thinking they have a relationship built on trust with the actor. This connection is used by the criminal, who may pose as the victim's grandchild or romantic interest, to influence the victim to:

- provide personal and financial information.
- give money or buy expensive gifts; or
- launder money unknowingly.

This particularly heinous cybercrime most commonly targets elderly women and those who are recently widowed.

REASONS FOR RAPID GROWTH OF CYBERCRIME

'Human beings are vulnerable, so rule of law is required to protect them' – Prof Hart said in his work "The Concept of Law". If we extrapolate this to the cybersphere, we may say that because of computers' vulnerability, the rule of law is necessary to defend and safeguard them from cybercrime. The causes of computers' susceptibility to attack include:

- **Easy access to everyone-** The difficulty in protecting a computer system from unauthorised access is that there is always a chance of a breach caused by complex technology rather than by human error. Key loggers that can steal access codes, sophisticated voice recorders, retina imagers, and other devices that can trick biometric systems and get beyond firewalls can be used to get past numerous security systems by being covertly implanted with logic bombs.

- **Negligence-** Negligence and human behavior are intimately related. Therefore, it is extremely likely that any negligence that occurs when safeguarding the computer system will allow a cybercriminal to access and take control of it.
- **Complex-** The human mind is flawed, thus it's unlikely that there won't ever be a mistake. The computers work on man-made programs which are commands/instructions which are composed of millions of codes. Sometimes user-friendly interface too has a lot of options and hidden tabs make the system operating tuff to handle.
- These holes allow the computer system to be breached by cybercriminals.

THE REMEDIES AVAILABLE FOR VICTIM OF CYBER CRIME

Cyber Crime complaint registration - Any of the following ways can be used by the victim of cybercrime to file a complaint:

1. National Cybercrime Reporting Portal (Online Cyber Crime complaint);
2. Cyber Crime Cell (Offline Cyber Crime complaint);
3. Local Police station (Reporting of cyber-crime)

However, The National Cyber Crime Reporting Portal has been the easiest and most practical way to file a complaint about cybercrime during the pandemic. The victim won't need to go to a police station or a cybercrime cell to complete the necessary paperwork or submit the proof.. The victim can easily file a complaint about the crime perpetrated against her using this way while sitting in her home. When filing a complaint, the pertinent evidence may also be uploaded to the Cybercrime Portal. Additionally, the victim will have the ability to monitor the progress of her complaint using the registered mobile number. Cybercrime offenses against women and children such as "Child Pornography, Child Sexual Abuse Material containing sexually explicit images/videos of children, sexually explicit content such as rape/gang rape" etc. can be registered by the victim/complainant on the Cybercrime portal. The relevant material may also be uploaded to the Cybercrime Portal when submitting a complaint. Additionally, using the registered mobile number, the victim will be able to follow the development of her complaint. Additionally, the victim or complainant has the option of registering the complaint anonymously, in which case their identify will not be made public. The victim/complainant must select the "Report and Track" option and register with a mobile number and email address in order to check on the status of the complaint in the future. With this choice, the victim or complainant will be promptly informed of any inquiries made and measures taken by the police officer in relation to the complaint filed.

The offline technique, in which the victim can send a written complaint to the closest cybercrime cell addressed to the Head of that particular cybercrime cell, is another choice available to the victim for the registration of a cybercrime complaint. The victim's name, contact information, postal address, and any further pertinent documents or evidence must be included with the complaint application.

If the victim or complainant does not have access to any of India's cybercrime cells, internet services, or devices, he or she may still register a FIR at a nearby police station with all the necessary details and supporting documentation.

Information Technology Act, 2000

Provides the provisions related to. Cybercrime as:

- **Section 66C** of the IT Act makes identity theft a punishable offence. "Instances of cyber hacking would be covered by this provision. Under this provision, whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

- **Section 66E:** Punishment for violation of privacy
  This section punishes the offender who intentionally or knowingly captures, publishes, or transmits the image of a private area of any person or a person engaged in private activities without the consent of such person.
  Punishment: Imprisonment which may extend to 3 years or fine which may extend to two lakh rupees, or with both.

- **Section 67:** Punishment for publishing or transmitting obscene material in electronic form
  This section punishes the cybercrime offender who publishes or transmits in the electronic form, any material which;
  1. Is lascivious (capable of arousing sexual desire), or

  2. It tends to deprave and corrupt the persons who are likely to read, see or hear the matter contained in it.
     Punishment: First conviction- Imprisonment which may extend to 3 years and fine which may extend to 5 lakh rupees.
     Second/subsequent conviction- Imprisonment which may extend to 5 years and fine which may extend to 10 lakh rupees.

- **Section 67A:** Punishment for publishing or transmitting of material containing the sexually explicit act, etc. in electronic form
  This section punishes the offender who publishes/ causes to publish or transmits/causes to transmit in

electronic form any material which contains sexually explicit act or conduct.

Punishment: First conviction- Imprisonment which may extend to 5 years and fine which may extend to 10 lakh rupees.

Second/subsequent conviction- Imprisonment which may extend to 7 years and fine which may extend to 10 lakh rupees.

- **Section 67B:** Punishment for publishing or transmitting of material depicting children in the sexually explicit act, etc. in electronic form

  This section punishes the offender who publishes/causes to publish, or transmits/causes to transmit, or creates text or digital images, collects, seeks, browses, downloads, advertise, promotes, exchanges, or distributes any material, in electronic form which depicts children engaged in a sexually explicit act or conduct. It also punishes the offender who cultivates, entices, or induces children to online relationships with one or more children for a sexually explicit act, or who facilitates online abusing of children, or who records in any electronic form abuse or sexually explicit act with children.

  Punishment: First conviction- Imprisonment which may extend to 5 years and fine which may extend to 10 lakh rupees. Second/subsequent conviction- Imprisonment which may extend to 7 years and fine which may extend to 10 lakh rupees.

Indian Penal Code, 1860

Related provision is like;

- **Section 354A:** Sexual harassment and punishment for sexual harassment

This section punishes the offender who commits any of the following acts-

1. Physical contact and advances involving unwelcome and explicit sexual overtures;
2. A demand or request of sexual favors; or
3. Showing pornography against the will of the woman; or
4. Making sexually colored remarks.

Any of the above-mentioned acts if committed with the use of the internet, computer device, or computer network, amounts to cybercrime and is punishable under this section.

Punishment: Imprisonment which may extend to 3 years, or fine, or with both.

- **Section 354C:** Voyeurism

This section punishes the offender who watches or captures the image of a woman engaging in a private act when she believes and expects not to be watched or observed by the perpetrator or any other person.

Punishment: First conviction- Imprisonment which shall not be less than one year, but which may extend to 3 years and fine.

Second/subsequent conviction- Imprisonment which shall not be less than 3 years, but which may extend to 7 years and fine.

- **Section 354D:** Stalking

This section punishes the offender who-

1. Follows a woman and contacts/attempts to contact such woman with the intention to establish a personal interaction despite clear indication of disinterest by such woman; or

2. Monitors the use by a woman of the internet, email, or any other form of electronic communication.

Punishment: First conviction- Imprisonment which may extend to 3 years and fine.
Second/subsequent conviction- Imprisonment which may extend to 5 years and fine.

- **Section 499**: Defamation

To defame a person is to do an act with the intention of harming the reputation of the person. Defamation by publication of visible representations of an imputation concerning the woman, when done with the intention to harm her reputation, is punishable with imprisonment for a term, which may extend to two years, or with fine, or both

- **Section 503**: Criminal intimidation

This section punishes the offender who threatens another with any injury to his person, reputation, or property with the intent to cause alarm to that person or to cause that person to do any act which he/she is not legally bound to do or to omit to do any act which that person is legally entitled to do.
Punishment under Section 506: Imprisonment which may extend to 2 years, or with fine, or with both. Punishment for criminal intimidation by imputing unchastity to a woman: Imprisonment which may extend to 7 years, or with fine, or with both.

- **Section 507**: Criminal intimidation by an anonymous communication

This provision provides the quantum of punishment for Criminal Intimidation when the same is by a person whose identity is not known to the victim. Any anonymous communication, which amounts to criminal intimidation under Section 503 stated above, is punishable under this section.

- **Section 509:** Word, gesture, or act intended to insult the modesty of a woman

This section punishes the offender who, intending to insult the modesty of a woman, utters any words, makes any sounds or gesture, or exhibits any object, or intrudes upon the privacy of such woman.
Punishment: Imprisonment which may extend to 3 years and fine.

The Indecent Representation of Women (Prohibition) Act, 1986

- **Section 4**: Prohibition of publication or sending by post of books, pamphlets, etc., containing indecent representation of women.

This section prohibits the production, sale, letting to hire, distribute, or circulation by post any book, pamphlet, paper, slide, film, writing, drawing, painting, photograph, representation, or figure which contains indecent representation of women in any form.

Punishment under Section 5: First conviction: Imprisonment which may extend to 3 years and fine which shall not be less than fifty thousand rupees, but which may extend to one lakh rupees.

Second/subsequent conviction**:** Imprisonment which shall not be less than 2 years, but which may extend to 7 years and fine which shall not be less than one lakh rupees, but which may extend to five lakh rupees.

Protection of Children from Sexual Offences Act, 2012

- **Section 11**: Sexual harassment of child and punishment therefore

Under this section, the sexual harassment of children has been defined. Sexual harassment of a child is said to be committed when the offender-

1. Utters any words, makes any sounds or gesture or exhibits any object or part of the body with the intention harass such child; or
2. Makes a child exhibit his body or any part of his body so as it is seen by such offender or any other person; or
3. Shows any object to a child in any form or media for pornographic purposes; or
4. Repeatedly or constantly follows/watches/contacts a child either directly or through electronic, digital, or any other means; or
5. Threatens to use, in any form of media, a real or fabricated depiction through electronic, film or digital or any other mode, of any part of the body of the child or the involvement of the child in a sexual act; or
6. Entices a child for pornographic purposes or gives gratification.

Punishment for sexual harassment of a child under Section 12: Imprisonment which may extend to three years and fine.

- **Section 13**: Using child for pornographic purposes and punishment therefore

Under this section, the offender who uses a child for sexual gratification, in any form of media (including Advertisement or Programme telecast by TV channels or internet or any other electronic/printed form), shall be guilty of the offense of using the child for pornographic purposes. The use of a child for sexual gratification includes-

1. Representation of sexual organs of a child;
2. Using a child engaged in real or simulated sexual acts (with/without penetration);
3. The indecent or obscene representation of a child.

Punishment under Section 14: First conviction- Imprisonment which may extend to 5 years and fine. Second/subsequent conviction- Imprisonment which may extend to 7 years and fine."

CONCLUSION AND SUGGESTIONS

The combating of the Cyber-crime can be done generally in three ways: Sensitization and awareness between the users, Use of Prevention and Detection tools, combating by the method of strong law and legislatures. Victimized community should directly contribute to the experience regarding prevention of the cyber-crime because the criminal strategies are absolutely new and mysterious trends of victimization. Now the need for some other gender related law that protects the common legal rights of women. Level of awareness of adult internet users of modern cyber cultures, Media interventions are the public awareness campaigns and other interventions delivered through television, radio, newspapers and other mass media. These can render an effective contribution in bringing about changes within the attitudes of the individuals towards gender norms. The media interventions are successful, when they seek to generate information in terms of the target audience.

There are some suggestive strategies to prevent Cyber-crime as;

- A significant contributor to crimes against women has been identified as sending private photos to friends and total strangers when chatting online. Avoiding such behavior is crucial.
- It is advised to avoid disclosing any personal information online in order to prevent cyber stalking.
- To minimize risks, remain up to date with technological and internet breakthroughs.
- Firewalls are an excellent first line of defense for stopping such intrusions. Make sure security checks are used safely. Always turn on the router's built-in firewall.
- It is prudent to maintain the privacy of the credit and debit card information at all costs. When in doubt about whether a transaction is real, verify with reputable sources
- Become familiar with the legal system and procedures related to such offences so that you can act quickly if you are ever caught.
- To ensure their protection and safety, empower and educate women and children and senior citizens with the necessary information and understanding about the prevalence of such heinous crimes in society.
- When dealing with such threats, use prudence and presence of mind. Avoid being a victim of fancies.
- The ideal strategy to combat these cybercrimes would be to take a cooperative perspective involving the ideas and actions done by the government and other legislative authorities to address such

crimes.

REFERENCES:

1. Section 43-75, Infotmatin and Technology (Amendment) Act, 2008
2. *Protection of Children from Sexual Offences Act, 2012*
3. *The Indecent Representation of Women (Prohibition) Act, 1986*
4. Gautam, R., Kulshrestha, P., & Goswami, M. A. K. (2021). Mediation And Family Dispute Resolution Mechanism: A Case Study On Clinical Legal Education. Elementary Education Online, 20(3), 2490-2490.
5. Gautam, R., "Proliferation of Cyber Crime and Indian legal system with special reference to Gwalior Division" Available at: https://shodhganga.inflibnet.ac.in/handle/10603/250817 Retrieved on: 22/07/2021
6. Pandey, N., Gautam, R., "property right of women in patriarchal indian society: a comprehensive study on legal narrative" Available at: https://www.researchgate.net/publication/361733554_PROPERTY_RIGHT_OF_WOMEN_IN_PATRIARCHAL_INDIAN_SOCIETY_A_COMPREHENSIVE_STUDY_ON_LEGAL_NARRATIVE_PROPERTY_RIGHT_OF_WOMEN_IN_PATRIARCHAL_INDIAN_SOCIETY_A_COMPREHENSIVE_STUDY_ON_LEGAL_NARRATIVE
7. Gautam, R., Medical health condition of prisoners and discrepancy in facilities among the states of Uttar Pradesh, Haryana and Delhi, International Journal of Health Sciences Follow journal, DOI: 10.53730/ijhs.v6nS6.12256
8. Gautam, R., Kanpur Philosophers ISSN 2348-8301 Vol IX, Issue V (IV), 2022151EFFICACY OF PROCEEDINGS OF CONCILIATION AND SETTLEMENT OF ANINDUSTRIAL DISPUTE UNDER INDUSTRIAL DISPUTES ACT, 1947, A CRITICAL Analysis. Available from: https://www.researchgate.net/publication/361733673_Kanpur_Philosophers_ISSN [accessed Sep 11 2022].
9. Gautam, Ritu, Cybercrimes and International legal regime, Available at: https://shodhganga.inflibnet.ac.in/bitstream/10603/250817/10/10_chapter-iv%20%20cybercrime%20issues%20and%20international%20legal%20regime.pdf
10. Gautam, Ritu, Cyber crime in India, Availablr at: http://hdl.handle.net/10603/250817

11.

9

JURISDICTIONAL CHALLENGES IN CYBERSPACE – A CRITICAL LEGAL ANALYSIS OF LEGAL THEORIES AND LAWS IN INDIA

KEYWORDS

PSYCHOLOGICAL FACTORS, CYBER FRAUD, CHILD PORNOGRAPHY,

CHAPTER NINE

JURISDICTIONAL CHALLENGES IN CYBERSPACE – A CRITICAL LEGAL ANALYSIS OF LEGAL THEORIES AND LAWS IN INDIA

AUTHOR

DR. DINESH DAYMA, ASSISTANT PROFESSOR OF LAW, CAMPUS LAW CENTRE, FACULTY OF LAW, UNIVERSITY OF DELHI, INDIA

ABSTRACT

Unlike the conventional world, the virtual world does not have territorial boarder, political barriers and territorial demarcation. The Cyberspace is the only place which devoid of any state/ country and boundaries. The global standards have converted the entire world into one group: One Global Place with extensive potential to exchange information with the help of highspeed. Cyberspace jurisdiction is an emerging area of internet because cyberspace lacks geographical boarder. Today's scenario world is facing the issue of internet jurisdiction due to different parties from different nations who have only virtual nexus with others. In the present world of internet, it is very difficult to find that where a

person really resides and where should be the cause of action arise in any case. The question arises whether business-related activity conducted over the internet - subject an individual or entity to personal jurisdiction in suits brought in another forum. When should a particular state or court excise personal jurisdiction over an Internet? Indeed, the biggest cryptic problem that evolved jurisprudence into the internet law is the fundamental issue of jurisdiction in the cyberspace. This article discusses contemporary case laws which is emerging jurisprudence on jurisdiction in cyberspace, focusing on U.S. and Indian court judgements addressing on this issue. This article also covers fundament principles to involving personal jurisdiction alongside test for determine jurisdiction in cyberspace. I furthermore address the concept of jurisdiction have accommodated with technological changes in the world. I additionally covering how Indian legislation define and address the concept of Cyber Jurisdiction in India.

INTRODUCTION

Jurisdiction is the vital essential feature of any nation's sovereignty. Jurisdiction of the state not only create, alter or terminate legal obligations but also restricts the intervene of another state in the internal matters of the state.[1] At present, Cyberspace has highlighted the jurisdiction concern in all nations. The exponential use of internet and with the ongoing globalization of e-commerce, trade and commerce continue to add importance of global framework for the jurisdiction. This innovative internet as well as cyberspace has not only raised the question of personal jurisdiction issue but also involved the international legal facet. The rapid growth of the various trade and commerce lead to exponential demand and use of the internet for the e-commerce which again highlighted the concern for the global jurisdiction issues along with need of the framework, recognition of the jurisdiction and its enforcement.

It's easy to resolve any kind of the complexity issue with the help of internet but on the other hand it re enforces the basic need for the global framework on the matter of jurisdiction and its recognition with enforcement in commercial as well as in civil matter. The main and important issue is that internet is that there is accessibility for everyone from everywhere. Whereas States (with physical borders) are the backbone of Public International Law, but Cyberspace is borderless.

The important issue- for public international law – that is the decisive for the states different Private international law or conflict of laws – is to decide where an online incident is occurring "in" or "outside" a certain state's jurisdiction pursuant to public international law. This issue has far from been decided yet.[2]

MEANING OF JURISDICTION AND PRE-REQUISITES OF JURISDICTION

The word "*Jurisdiction*" means that the court has power to adjudge any case.

[1] Malcolm N. Shaw, *International Law* (5thedn, Cambridge University Press 2003) 452-54.

[2] The European Cybercrime Convention is totally silent on this vital issue.

If in any case a court dearth its jurisdiction then its judgement has no effect in law. Jurisdiction can be divided in two categories namely;

1. *Subject matter Jurisdiction*
2. *Personal Jurisdiction*
3. *Pecuniary Jurisdiction*

This above mentioned three jurisdictions should be complied if the court passes the judgment that is enforceable. Most important is the subject matter jurisdiction. It empowers the court to entertain limited and certain type of cases. The categorization is must to avoid the piling up of cases in the court of law. The forums have the power only to hear the cases of their own subject matter jurisdiction or domain. This power cannot be transgressed.

A civil court cannot hear criminal matters and *vice-versa*. "*Personal Jurisdiction*" is that in which the court has the power to hear and to decide in a case where a set persons involved.

Meaning thereby, the accused must be of the same place where the forum has its territorial jurisdiction.

This means against any person whom a case is filed should belong to territorial jurisdiction in which that particular forum is situated. "Pecuniary Jurisdiction" inculcate the amount of money claimed in the legal proceeding. The pecuniary jurisdiction of a court is divided in hierarchical order. To make a judgement valid and enforceable there are three pre-conditions that needs to be satisfied, namely:

1. The Jurisdiction to prescribed

2. The Jurisdiction to adjudicate, and

3. The Jurisdiction to enforce

As per the rules of international law, a nation has authority to enforce its jurisdiction on non-citizens also that may have interest in their state but this is restricted in nature. There are many cases where a non – citizen may transact business (online) and continue his business from that country where he does not even reside.

In different cases a non-citizen may transact online business and do business in forum state where he does not reside.

Different countries have developed different principles that apply in similar situations to determine jurisdiction such as:

1. **The Jurisdiction to Prescribe:** When the laws are applicable to a certain category of persons, it is the jurisdiction to prescribe. It is basically, the power of the state to enforce its laws on persons, their actives and the interpersonal relationship and business or other entitlement in the States.

In USA the Restatement (Third) of Foreign Relations Law of United Nations, 1987,[3] mentions that country has

[3] The Restatement (Third) of Foreign Relation Law (1988).

the jurisdiction to prescribed laws., it will have "jurisdiction to prescribed law with respect to-

(1) conduct that, wholly or in substantial part, takes place within its territory;
(2) the status of persons, or interests in things, present within its territory;
(3) conduct outside its territory that has or is intended to have substantial effect within its territory;
(4) the activities, interests, status, or relations of its nationals outside as well as within its territory; and
(5) certain conduct outside its territory by persons not its nationals that is directed against the security of the state or against a limited class of other state interests".[4]

These principles are also famous as territorial principles, nationality principles, the effect principles and the protective principles, respectively. The board criteria are assuming jurisdiction has to be exercised on parameters of reasonableness as stated by Restatement (Third) of Foreign Relation Law, 1987.

2.**The Jurisdiction to Adjudicate**: The forum is empowered to make the decision related to a person or a thing. To apply this, a nation needs to have the jurisdiction to prescribe the law that is required to decide the related dispute. Now, there arises a question to ascertain the jurisdiction for non-resident persons. There are many reasons that are taken into account while deciding the jurisdiction that is applicable to take up the matter. It is pertinent to note that if it is determined that the jurisdiction is reasonable, it need not to have the laws related to the jurisdiction to prescribe. The jurisdiction to adjudicate is missing, while the jurisdiction to prescribe is certainly present. For example, under Section 1(2) of the Information Technology Act, 2000, if read along with Section 75 enumerates that the applicability of the said act. Meaning thereby, the offences are triable under the act that are committed outside the territorial limits of India. According to Section 75 of the same act, if any offence is committed by a person (of any nationality) outside India, such an offence will be triable under this act.[5] These notable sections ensure that prescriptive jurisdiction is in existence on the non-Indians also, irrespective of the fact that such an offence is committed outside India. But the major issue is to ascertain the jurisdiction. In this context, the concept of extradition may arise. The person needs to get extradited, if there is a treaty in existence between those two nations. In many cases, it has been observed that the non-residents do not comply to the jurisdiction of the regulating state.

3.**The Jurisdiction to enforce**: Jurisdiction plays a vital role in every kind of offence. It means the power of the state to take any action including judicial or non-judicial, as the case may be, to enforce its rules and regulations on that person. The state has the power to impose the punitive provision on the accused.[6] This condition is applicable only if a State has the jurisdiction to prescribe. Under the Code of Civil Procedure[7] (CPC), the judgment of the foreign court is considered to be conclusive subject to the provision that the judgment is not passed by the competent court or is not made on merits of the case.

Another case may also arise that, if the applicability of international law is not made properly or it does not follow the Indian laws. Indian courts will not recognize a foreign judgement also where proceeding took place in violation of natural justice, or judgement was obtained by fraud or sustain a claim based on breach of any

[4] The Restatement (Third) of Foreign Relation Law (1987) s. 402, 403 & 421.
[5] The Information Technology Act, 2000 (Act 21 of 2000) s.75.
[6] The Restatement (Third) of Foreign Relation Law (1987) s. 401, 403 and 421.
[7] The Code of Civil Procedure, 1908 (Act 4 of 1908) s. 3.

Indian laws. These facts prove that there is demand of making contraventions and treaties at international level. The absence of which, may result into increase in cybercrimes. Enforcement mechanism, by and large involves different actions, including police investigations, service of court orders and arrest of suspected persons.

JURISPRUDENTIAL EXPANSION OF JURISDICTION IN INTERNET

The Long Arm Statutes

The enactment of long arms statutes allowed the local courts to exercise personal jurisdiction over non-resident as long as it complies with the principles of due process elucidates in 14th Amendment of Constitution of United States. In *Hess v. Pawloski*[8] the Supreme Court of United States upheld a Massachusetts status that provided that non-resident who use the roads in Massachusetts would be deemed to submit to jurisdiction in Massachusetts as legally valid. However, in the case of *United State v. Thomas*[9] , a criminal action was filed against person who posted obscene massage on bulletin board systems that were accessed by subscription in Tennessee violation the federal laws. It was held that because the defendant had knowingly sent their material into Tennessee by accepting a subscription from resident of that state. It was justified to use the community standard of Tennessee to check criteria to determine the obscenity images. The court observed "*Venue for federal obscenity prosecution lies*" in any district from, through or into which allegedly obscene material moves.

Minimum Contacts Test

In *Washington v. International Shoe Company*[10], the United States Supreme Court explained the Minimum Contracts Test. According to this test, a State can sue a non-resident Foreign Corporation if the Corporation satisfies the "*minimum contact*" with the foreign state and principles of justice and fair play been duly considered. "*minimum contact"* means physical contact or presence within Forum States.

The Effect Test

The concept of effect test originated by the Supreme Court in the case of *Calder v. Jones*[11] *in* 1984, described as where a state derives personal jurisdiction over a non-resident person.

An article in National Enquirer written by Florida residents who were not associated with California, defamed Jones in their article. He was a popular movie actress of California. The Supreme Court in a relatively brief opinion found jurisdiction, holding that California was "*the focal point both of the story and the harm suffered*." In doing do, the court felt that it is forced to differentiate its earlier decisions which held the "foreseeability" of the impact in the forum. The court also held that the there is a need to ore forceeability of instant facts. The defamatory articles were sufficient to prove the defendant's action as "*aimed at California*": defendants have the knowledge that their article would have a "*potentially devastating impact*" on the plaintiff and that "the brunt of

[8] 274 US 352 (1927).

[9] 74 F.3d 701 (6th Cir. 1996).

[10] 326 US 310(1945).

[11] 465 U.S. 783 (1983).

that injury" would be assessed by her in California, therefore the defendants has the knowledge of appearance in California court.

In this case court also derived four grounds to determine jurisdiction. "First, the case involved defamation, the gravamen of which is damage to a person's reputation in the community." The "community" is an important point to define the tort. Second, in California, the major element to constitute an offence of libel is the malice intention. In context of the public figure, the defendants were accused of acting, "maliciously and with intent to injure, defame and disgrace Jones and cause her to suffer humiliation and emotional and physical distress." Third, everyone who is an active participant in the defamatory publication is said to commit an offence of libel. Fourth, one of the facts that was not mentioned by the California court is that the National Enquirer's largest seller of California, where 600,000 copies ("twice the level of the next highest state") were sold. Furthermore, the court also refer the case; in 1998, in *Panavision International v. Toeppen*[12], the court reiterated the 'effect test' in a case concerning and Illinois resident. Toeppen engaged in a cybersquatting activity by registration to Panavision. The court held that California had specific jurisdiction over non-resident Toeppen. The court took the view that Toeppen knew that Panavision would feel the effect of his illegal action in California as its principal office was located there. Toeppoen had never visited California or since the effect of his action in Illinois were left in California, the exercise of personal jurisdiction by California Court was justified.

INDIAN LAWS TO DETERMINE JURISDICTION

The Code of Civil Procedure 1908, Information Technology Act, 2000 And Jurisdiction

In India like many other countries, has a deep rotted legal infrastructure and at the same time it has increasing convergence. The result is that India too is sharing the legal cacophony which is the outcome of the technological boom. The difficulties of being a part of the ancient society overshadowed by the blues of the information society are hard to quantity at the moment. The basic principles of jurisdiction as recognised by the world over are well received in India in the Civil Procedure Code, 1908 (CPC) and the Criminal Procedure Code (CrPC),1973.[13]

The Criminal Procedure code (CrPC) is a time-tested law and envisages the basic rules of jurisdiction which are contained in Chapter XIII CPC from Section 177 to 189.[14] Section 177 contains the basic rule of criminal jurisdiction and read thus,

> Section 177.*Ordinary place of inquiry and trial*: - Every offence shall ordinarily be inquired inland tried by a Court within whose local jurisdiction it was committed.

This rule originally constructed about a century ago is rightly regarded as one of expediency.[15] The wording

[12] 89F 3d 1257 (6th Cir 1996).

[13] Talat Ftima, *Cyber Crimes,* (2nd ed. EBC 2016) 510-11.

[14] The Code of Civil Procedure, 1908 (Act 4 of 1908) s 156. The Code makes these general rules applicable for deciding which shall be the proper police station to entertain investigations into an offence.

[15] K.N. Chandrasekharan Pillai, *R.V. Kelkar's Lectures on Criminal Procedure*, 141 (3rd edn, ECB 1993) 140.

of the 41st Report[16]depict the mind of the legislators who cared so much for the convenience of the accused.

> Considering the size of the country, the distance of courts from the place of crime and difficulties of transport in the interior, it would seem expedient and desirable that the inquiry and trial should ordinarily take place in the vicinity of the crime.

These wording when being repeated today show how drastically the world has undergone a change and so have the practical considerations. If the wording is seen in the context of the internet, the legislators will now have to consider the size of the cyberspace, the distance of courts from the place of crime now running into thousands of miles; and the vicinity of crime expanding globally. This section appears to be an antique piece of law, is still successful in the physical world whereas in India not much has changed for the common man since. In present situation it was plausible for legislation to know that a crime cannot be sole act and can either be committed in instalments or it ramifications may go beyond the place of commission of crime, thus Section 177 stated the term "*ordinarily*" to denote that the rule shall govern all criminal trial held under the CrPC including trials of offences punishable under local or special law.[17] Thus rule under the section is neither exclusive not peremptory[18] as it is subject to the other provisions of the CrPC.

APPLICATION OF CRIMINAL LAW ON JURISDICTION

Even in the offline world, a century back, "uncertainty" regarding place of jurisdiction did exist and hence, section 178 was enacted "in order to prevent an accused person from getting off completely because these might be some uncertainty and doubt as to what particular court has the local jurisdiction to inquire into or try the case".[19] Usually the place of inquiry or trial is ascertained also on the basis of averments made in the complaint or police report. As the application of the CrPC is to the territory of India, it is limited to the territory of India with few exceptions as mention in section 1(2).

The CrPC is the backbone of all the criminal proceeding which are held in the country but there is ample scope for accommodating some specific provisions given under some other law of the country if it provides.

The applicability of legal rules to crimes committed in cyberspace is the interplay of several Acts. In US also the pre-internet rules and regulations of jurisdiction, which emanate directly from, its constitution, are being applied in matter of Internet jurisdiction. In the real world too, lawmakers were confronted with a situation where the commission of crime tool place in one area while its effect was seen in another area and the accused was recovered from a totally different area. Aging there are offences which are protracted to a gathered length of time and place. Apart from dealing with the offences committed within India, the CrPC also supplements section 4 of the Indian Penal Code, which contains the extension of the IPC to extraterritorial offences. Sec-

[16] Vol. I, 84, Para 15.13.

[17] *Narumal v. State of Bombay,* AIR 1960 SC 1329, 1332:1960 Crj L J 1964.

[18] K.N. Chandrasekharan Pillai, *R.V. Kelkar's Lectures on Criminal Procedure*, 141 (3rd edn, ECB 1993) 141.

[19] *DebendraNathDas Gupta v. Registrar of Joint Stock Companies*, ILR (1918) 45 Cal 490; *PunardeoNarain Singh v. Ram Sarup Roy,* ILR (1898) 25 Cal 858,860, 862-63.

tion 4 of the IPC says:

1. (Amended)[20] "The provisions of this Code apply also to any offence committed by-
   (1) any citizen of India in any place without and beyond India;
   (2) any person on any ship or aircraft registered in India wherever it may be;]
   (3) any person in any place without and beyond India committing offence targeting a computer resource located in India.]". 1

Explanation- In this section-

(a) the word "offence" includes every act committed outside India which, if committed in India, would be punishable under this Code;
(b) the expression "computer resource" shall have the meaning assigned to it in clause (k) of sub-section (1) of section 2 of the Information Technology Act, 2000.]

Section 2(1)(k) of the Information Technology Act says,

> "Computer Resource means computer, Computer system, computer network, data, computer database or software".

The extraterritorial extension of the CrPC is divided on two parts, *Firstly*, it concerns the person or the citizen of India and *secondly*, it concerns the place, namely the aircraft and ship. In either case the CrPC is applicable to the situation as if it is applied in Indian surroundings. The amendment to the section meant to make it suitable for internet situations. It is a known fact that cybercrimes are borderless crimes, they have defined the fundamentals of jurisdiction yet they cannot be ignored by saying that. Hence, it has been that effort of lawmakers to deal with the law according the new dimension. Section 4 of the IPC has been amended accordingly. The newly added provisions sub-section (3) gives importance to the place where the "computer resources" is situated. While sub-section (1) gives importance the "person" or "citizen" and sub-section (2) gives importance to the vessel registered in India, on the same principle, the place where a computer resource, namely, the *extraterritorial principle* embodied in the section.

An analysis reveals that a person, no matter whether he is or to whatever country he belongs, if his movement at the keyboard makes a change or affects any computer resources in India in the form of an offence then the CrPC will extend to him.

In this situation, the procedural counterpart of the law given in the Section 188 and 189 of the CrPC comes into play. Section 188 says,

188. "*Offence committed outside India*: - When an offence is committed outside India-

(a) by a citizen of India, whether on the high seas or elsewhere; or
(b) by a person, not being such citizen, on any ship or aircraft registered in India,

[20] Amended by virtue of S. 51 of Information Technology (Amendment) Act, 2008 (10 of 2009) – Af ter sub-s. (2), new sub-s. (3) is added.

> he may be dealt with in respect of such offence as if it had been com- mitted at any place within India at which he may be found:
>
> Provided that, notwithstanding anything in any of the preceding sections of this Chapter, no such offence shall be inquired into or tried in India except with the previous sanction of the Central Government".

A comparison of section 4 and 188 as mentioned would reveal that section 188(1) is a logical and procedural supplement to section 4(1) while section 188(2) is a logical and procedural supplement to section 4(2). The word "found" in section 188 has varied interpretation in the case of *Empress v. Manganlal*[21]*,* the court says that the word "found" does not mean where the person is discovering but where he is actually present. While in several cases including *Emperor v. Vinayak Damodar Sarvarkar*[22], it was held that when an offence is committed beyond India then the accused can be tired at any place where he is found irrespective of the fact that such accused comes voluntarily or in answer to summons or under illegal arrest. It is enough that the court should find him present when it comes to take up the case.[23] Along with these two provisions, the law of Extradition Act, 1962 also comes into play. This is further elaborated by the new clause added to the Explanation of section 4 of the Indian Penal Code which gives the meaning of the word "computer resource" as per the definition given in section 2(1)(k), IT Act, 2000 thereby making it suitable for transnational crimes. The amended section gives jurisdiction to the Indian courts if the affected computer resources is situated in India. The procedure to be followed is as given under section 188 of CrPC. The combined rules given under these two sections depict the legitimate right of a sovereign state on its citizens, not only on its lands but also beyond it, any foreign land.

However, the code or civil procedure, 1908 prescribes pecuniary jurisdiction limiting the power of the court to hear matter up to a particular pecuniary limit.[24] As per Section 16 of the Code[25] "the jurisdiction in case is also determined to the criteria of where the subject matter is situated". Where a suit is for a tortuous act committed in one jurisdiction and the defendant resides in a different jurisdiction, suit may be instituted in either jurisdiction at the option of the plaintiff. [26] In other case jurisdiction lies where the defendant actually and voluntary resides, or carries on business, or personally works for gain or cause of action, wholly or partly arise.[27] In *Rajasthan High Court Advocate's Association v Union of India*[28], the Supreme Court interpreted the term cause of action as every fact necessary for the plaintiff to prove, if traversed, in order to support his entitlement to the judgement of the court. According to the court, each fact which is necessary to prove (different from each piece of evidence which is necessary to prove every fact) constitutes the cause of action.

On the other issue of jurisdiction, the Information Technology Act, 2000 provides in clause 2 of Section 1 of the Act[29], extended the whole of India and applies also to any offence or contravention thereunder committed

[21] ILR (1882) 6 Bom 622.
[22] ILR (1911) 35 Bom 225.
[23] *SahebraoBajirao v. SuryabhanZiblaji*, AIR 1948 Nag 251; 49 Cri LJ 276.
[24] The Code of Civil Procedure, 1908 (Act 4 of 1908) s 6.
[25] The Code of Civil Procedure, 1908 (Act 4 of 1908) s 16.
[26] The Code of Civil Procedure, 1908 (Act 4 of 1908) s 19.
[27] The Code of Civil Procedure, 1908 (Act 4 of 1908) s. 20.
[28] 2001 (2) SCC 294.
[29] The Information Technology Act, 2000 (Act 21 of 2000) s.1.

to an offence outside India by any person. Further, Section 75(2)[30] states that the Act applies to an offence or contravention that involves a computer, computer system, or computer network located in India. This provision conferred a prescriptive jurisdiction on Indian courts whereby of any objectionable material that illegal as per the Information Technology Act is accessible by computer located in India, it shall constitute an offence. Such a provision gives wide sweeping power on the Indian courts to assume jurisdiction overran out of state defendant that may exhibit any information or conduct activates through its website which are perfectly legal in its country but violates Indian Laws. The difficulty lies also in enforcement of the judgement passed by a court when it adjudicates a matter (in most cases *ex-party* as the court out of state defendant often challenges the lack of jurisdiction or does not participate in the matter). We need to adopt a clear approach for determining jurisdiction to deal with cyberspace between parties involving two or more jurisdictions. However, India being a signatory to the Model Law has accordingly embarked upon cyber legislation and came out with its hitherto sole cyber legislation, the Information Technology Act, 2000. Section 75[31] envisages bot subject matter and territorial jurisdiction. The section applies to offences and contravention not only committed in India. Thus, it means that the section is having extraterritorial application, something badly required in this borderless world. It means that this feature of it is similar to the long arm statutes of the states of the US.[32]

CONCLUSION

The cyberspace is far away from the boundaries of territorial jurisdiction. there can be more than one jurisdiction where the disputes concerning the citizens are in question.

As far as the utopian homogeneity in law is concerned (if at all it is considered possible) and a universal forum to settle cyberspace disputes is established, one must have to comply on the personal jurisdiction ascertained by the courts to resolve the disputes offline. It is interesting to think of a situation where offline disputes while arriving at this point I think this will be an impossible task as more and more offline activity is shifting its medium to online activity. In fact I can visualize a situation where humans can do nothing without computers in the near future. The conventional offline courts may be substituted with online forum which decide disputes based on homogenous laws and float universally in cyberspace not belonging to a particular territorial jurisdiction. There are such criminals also, who use the technologies to commit more advance and serious crimes. All the three pillars i.e. Legislatures, Executive and Judiciary are trying to combat these crimes. In the end, the society is the victim of such crimes. The society is afraid of the new technologies being introduced; they are presumed to be misused by the criminals. They have faith on the judicial system, that they will be protected by the law. The cyber-crime should be handled strictly. The justice system needs to be more powerful to make stringent laws and regulations to reduce cybercrime. The IT Act, 2000 is established to reduce this crime, but the proper implementation is somewhere missing. Now is the correct time for such implementation only then we can expect the safer environment for our generations.

[30] The Information Technology Act, 2000 (Act 21 of 2000) s. 75(2).

[31] The Information Technology Act, 2000 (Act 21 of 2000) s.75.

[32] Nandan Kamath, *Guide to Information Technology and Rule*, (2ndedn, Universal Law Pub., 2001) 52.

10

AN ANALYTICAL STUDY ON CYBER CRIME AGAINST CHILDREN

KEYWORDS

NCRB - NATIONAL CRIME REPORT BUREAU, IPC - INDIAN PENAL CODE, IT ACT - INFORMATION TECHNOLOGY ACT

CHAPTER TEN

AN ANALYTICAL STUDY ON CYBER CRIME AGAINST CHILDREN

AUTHORS

DR. NEETI PANDEY, PRINCIPAL, MADHAV VIDHI MAHAVIDALAYA, GWALIOR, INDIA

SOURABH SHARMA, RESEARCH SCHOLAR, JIWAJI UNIVERSITY, GWALIOR, INDIA

ABSTRACT

The Internet has become the most powerful channel for communication in recent years. In this time of pandemic, it has taken place in the lives of everyone in a variety of forms such as education, communication, business, social networking, online shopping, and online transaction, etc. During this pandemic period, children are more exposed to online networks, and these factors lead to create possibilities for predators to commit cyber crime against children. During this time, children are more likely to be targeted by cyber criminals. According to statistics that was just released by the NCRB, there has been a significant increase of 400 times in the amount of cyber crime committed against minors in the past year. These can take many forms, including phishing, grooming, child pornography, and others like them. It is true that these crimes are only reported once, but it is also true that the vast majority of cyber crimes go undetected since victims only disclose them after the situation has grown more problematic for them. Even though the government has taken a number of different pre-

ventative measures and released a number of different guidelines, there has been an increase in the number of online crimes committed against minors.

The purpose of this research paper is to examine the current trend of cybercrime committed against children, as well as different associated laws and measures taken by the government, as well as several protections to prevent cybercrime against children. This research is also carried out in order to develop acceptable answers to the problem of cybercrime committed against minors.

INTRODUCTION

Cybercrime is currently the most challenging issue facing the world of the internet at the present time. The term "cyber crime" refers to any unlawful activity that is carried out primarily via the use of the internet. During this period of covid time, precautions were made to limit the spread of the pandemic, which ultimately resulted in the closure of schools and caused a push toward virtual learning settings. Children started spending more time online for purposes of pleasure, social interaction, and education, but they were not always aware of the potential problems that were involved with this trend. Children are more likely to be vulnerable to a variety of risks, including sexual abuse, grooming or sexual solicitation, sexting, exposure to pornography, production and circulation of child sexual abuse material, cyber-bullying, online harassment and cyber-victimization, and many other privacy-related risks. Children are also more likely to be bullied. According to a study published by UNICEF in 2020, it was projected that during the Covid pandemic about 37.6 million children across 16 states in India completed their education by participating in a variety of remote learning initiatives such as online classrooms and radio programmes. Children's mental and social health has suffered as a result of the restricted opportunities they have had to interact with others during periods of lockdown, evacuation, and school closures. The experts also revealed that the Covid period causes an increase in loneliness, mood to conduct disorders, substance abuse or anxiety disorders, and that all of these factors cause an individual to use the internet compulsively, access objectionable content, or simply be more vulnerable to being bullied or abused. In addition, experts believe that parents, teachers, and members of society have a poor grasp of children's interactions with information and communication technologies (ICTs) and the perceived threats that they encounter online. The vast majority of youngsters, particularly those who are in grades one through five, have a very little understanding of how to responsibly use technology and the internet, as well as ethical considerations. As a result, it is quite simple for anyone who want to exploit young children sexually or do other forms of cybercrime to hack into the gadgets that they use and exert control over them. A youngster does not know whether or not a specific website is safe to visit, or whether or not a particular image or video should be downloaded, and as a result, they are easily led astray to participate in immoral acts and become easy targets for those who engage in cybercrime. It is important for parents, teachers, and other adults who care for and educate children to have an understanding of what children need to know in order to be able to direct them in an acceptable and responsible manner. The currently available awareness development programmes are disjointed, lack a unified content emphasis, and have a restricted audience base.

According to statistics that was just released by the NCRB, the rate of crime committed against minors is expected to increase by a factor of 400 in the year 2020. The most significant increase was observed in child pornography, with 738 reported cases out of a total of 1102 cases of cyber crime committed against children. This was followed by cyber stalking and cyber bullying, with 140 reported cases, and other cyber crime committed against children, with 220 reported cases. Recent research has shown that cyber criminals nowadays target youngsters for the purpose of committing cybercrime. These crimes include sexual extortion, online fraud, e-sim fraud, and game bullying. Among them, sexual extortion is on the rise at an alarming rate. According to the findings of the survey, the most common reason for perpetrating a cybercrime in the city is to perpetrate fraud. There were further cases involving personal revenge (83 total cases), bringing discredit (362 total cases), sexually explicit content (89 total cases), political retribution (5), and several other types of crimes. (2) According to statistics provided by the National Crimes Record Bureau, the states with the highest number of reports of cyber crimes committed against minors are as follows: Uttar Pradesh (170), Karnataka (144), Maharashtra (137), Kerala (107) and Odisha (71).

Because of their reputation and their fear of their families, children almost never disclose these types of offences, which is one of the primary reasons why these crimes go undetected. This is another finding from an examination of cybercrime. As a result, these items demonstrate that this data is a very huge one in the actual sense. Previous research also leads us to believe that the majority of this information comes from urban regions, as victims in rural areas are less likely to disclose such incidents. The increase of such crime is also largely due to the widespread lack of awareness regarding cybercrime, the preventative measures that should be taken, and the laws that should be enforced. The government has undertaken a number of efforts, such as those in which it offers a variety of preventative measures and protections, in order to reduce the incidence of cybercrime against minors. In addition to this, the government has launched a number of different campaigns to promote people's awareness of cyber crime. To combat this type of criminal activity, the government has launched a number of different initiatives, such as the "Masum" programme in Delhi. In addition, many amendments have been made to the Indian Penal Code and the Information Technology Act, and the POCSO Act has been implemented in order to protect minors from being victims of cybercrime. The legislation has resulted in the passage of the POCSO Act and the provision of stringent punishments for cybercrime committed against children. Despite the fact that we have a variety of guidelines to report such crimes and many forms of law that is effective, but in this case we need to be more conscious of such crimes, and we need take all preventive measures to avoid such crime from occurring. As a result of the fact that children are more exposed to the internet for the purposes of education, communication, and gaming in today's world, it is imperative for parents to keep a close eye on their children whenever they use the internet. Since the internet is now an integral part of our lives, and since we are unable to conceive of doing anything else in its absence, it is imperative that we take preventative precautions and file reports regarding any criminal activity that may occur. We need to educate our children about the precautionary measures that should be taken when using social networking sites and the internet, and we also need to inform them about the harmful effects that such a crime can have, such as the effect it has on a person's reputation, social image, and friends, among other things. This has the potential to be a useful weapon in the fight against crime committed against children. The expert also emphasised the necessity of a coordinated approach to the task of preparing children, caregivers, teachers, and the general public with the skills necessary to protect themselves from any dangers posed by the internet and to act as responsible digital citizens. Children are now much more at risk as a result of the epidemic since they are forced to interact with the internet world for the purposes of their education. This leaves them feeling helpless. The vast majority of children, particularly those in grades 1 through 5, have a limited amount of experience with technology, appropriate internet behaviour, and ethical considerations related to their use of the internet. As a result, it is relatively simple for anyone who are interested in sexually exploiting children or committing other forms of cybercrime to hack the electronic devices that these youngsters use and to exert control over them. A youngster does not know whether or not a specific website is safe to visit, or whether or not a particular image or video should be downloaded, and as a result, they are easily led astray to participate in immoral acts and become easy targets for those who engage in cybercrime.

CRIMES COMMITTED ONLINE AGAINST CHILDREN

Children were using the internet and other virtual platforms for educational purposes, but they were ignorant of the risks that were associated with doing so. At the same time, children were being exposed to cybercrime offenders because they were the easy targets to manipulate and harass. The children were forced to helplessly rely on these virtual platforms for the fulfilment of the educational needs of the children, which left the children vulnerable to being manipulated and harassed. During the pandemic, some of the most prevalent types of cybercrimes that were performed against children while they were participating in activities that were either instructive or entertaining include the following:

Sexual abuse of children

These child sexual abuse materials include child pornographic photographs and films, online sexual exploitation of children by phone call or video chat, in which children are compelled into performing sexual activities, and other forms of media depicting sexual activity involving children.

Pornographic/sexually explicit content for children

While children are using the internet for educational and entertainment purposes, or while they are browsing a social media page, they are being encouraged to open certain websites that direct them to sexually explicit content and pornographic videos and images. These websites are known as "clickbait." The child's mind will be permanently damaged as a result of this, but the criminal will get popularity and financial reward.

Cybersex trafficking

In cases of cybersex trafficking, the victim does not have any face-to-face interactions with the person who is abusing them. During the process of cybersex trafficking, the dealer either live-streams, films, or takes photographs of the victim engaging in sexual or personal actions in a central place, and then sells the content online to sexual predators as well as customers. Children have been subjected to sexual abuse at the hands of the perpetrators, who have forced and manipulated them into participating in a cybersex trafficking operation.

Cyber bullying

This includes remarks and communications that are nasty, mean, abusive, or harmful in any other way against the child victim. Children are easy targets for bullying due to the fact that they are naturally naive, and it is even lot simpler for those who engage in bullying behaviour to target children on virtual platforms. Children who are victims of cyberbullying are more likely to engage in behaviour such as avoiding school classes through the use of virtual platforms, suddenly wanting to stop using the internet and computer devices, maintaining a secretive attitude regarding their digital life, as well as experiencing distress and emotional instability.

Child grooming

The perpetrator of the crime makes the young victim feel comfortable around them by developing an emotional and trusting relationship with them in order to carry out their plan to sexually abuse the child. Because children have a propensity to trust easily, it is quite simple for those who commit crimes to form a connection with them and exploit that trust. Once a connection has been established, the offender will begin to exert control over the youngster in order to coerce the child into engaging in sexual actions. During the epidemic, one of the most common types of cybercrime that was performed was the grooming of children through various internet platforms and social media. Child predators were able to operate and acquire the confidence of children online, and they were able to do so with relative ease as a result of the lack of understanding among both children and their parents regarding the potentially harmful aspects of the internet.

Some of the most notorious online crimes perpetrated against children during the epidemic are those that have been highlighted above. Crimes like this have been committed against children and their parents, making both groups of people victims. This highlights the need of educating both children and their parents about the online world and the steps they should take to safeguard themselves from individuals who engage in criminal activity online.

TREND ANALYSIS OF CYBER CRIME AGAINST CHILDREN

The most recent statistics from the NCRB reveals that there has been a significant rise in the amount of cybercrime committed against minors during this covid time. In 2017 there were a total of 88 cases of cybercrime committed against children, 232 cases in 2018, 305 cases in 2019, and 1102 cases in 2020, as shown in table 1, if we analyse the data from the NCRB relating to cybercrime committed against children from 2017 to 2020, then we find that in 2017 there were 88 cases of cybercrime committed against children. The numbers presented here make it abundantly evident that there would be a rise in the incidence of cybercrime committed against minors throughout the period covering 2019 and 2020 of more than 361,100 percent. When we do detailed research on the many forms of online crime committed against minors, we discover that there has been a significant rise in the production of cyber pornography. According to the data collected in 2017, the most common types of cybercrime committed against minors were cyber pornography (7 instances), internet stalking/bullying (7 cases), and cyber blackmailing (1). There was just one occurrence of cyber blackmail in 2017. According to data from the NCRB for 2018, the number of cases involving phoney profiles and cyber stalking decreased to three and zero, respectively, while the number of cases involving child pornography increased to forty-four. In a similar vein, the data collected by the NCRB in 2019 reveals that the number of instances involving child pornography was high, totalling 102, while the number of cases involving phoney profiles and cyber stalking was low, totalling 1 and 1 respectively. In conclusion, the statistics from the NCRB for 2020 reveal that, similar to the data from 2018 and 2019, the number of cases involving child pornography was high, with 738 instances, while the number of cases involving phoney profiles was similarly low, with only one case, as shown in table 2.

Table :1

Year's	Cyber Cases	Percentage increase
2017	**88**	**153**
2018	**232**	**263.63**
2019	**305**	**131.46**
2020	**1102**	**361.31**

Table :2

Crime Head wise cases of cyber crime against children						
Sr. No.	**Crime Head**	**Year**				**Persentage variation in 2020 over 2019**
		2017	**2018**	**2019**	**2020**	
1	Cyber Black mailing /Threatening / Harassment	1	4	3	3	0.0
2	Fake profile	3	3	1	1	0.0
3	Cyber Pornography	7	44	102	738	723.5
4	Cyber Stalking	7	40	45	140	311.1
5	Internet through online Games	0	0	1	0	0.0
6	Other cyber crime against children	70	141	153	220	143.8
	Total	**88**	**232**	**305**	**1102**	**361.3**

PRESENT LAWS TO CURB CYBER CRIME AGAINST CHILDREN

The legislative body has taken a number of steps to strengthen the penalties for online crimes committed against minors. The government has passed a number of legislations, such as the POCSO Act and the IT Act, all of which contain provisions that can be used to effectively penalise those responsible. The following are some of the provisions that are mentioned below:

"2012 legislation titled the Protection of Children from Sexual Offenses Act."[1]

Section 11: Sexual harassment of children and the consequences for those who do it

The term "sexual harassment of minors" has been given its own definition in this section. When a kid is subjected to sexual harassment, it is considered to be a crime if the offender:

- Compel a youngster to expose his body or any portion of his body to a criminal or any other person in such a way that they are able to view it; or

- Exposing a child to pornographic material in any way, shape, or form, or doing so with the intent to do so; or

- Repeatedly or consistently follows, watches, or makes contact with a kid, either directly or by any other means, including but not limited to electronic, digital, or any other means; or[2]

- Threatens to use, in any form of media, a real or fabricated depiction through electronic, film, or digital or any other mode of any part of the child's body or the involvement of the child in a sexual act; or threatens to use any form of media to use a real or fabricated depiction of any part of the child's body or the involvement of the child in a sexual act.

- Encourages a youngster to engage in pornographic activity or provides the child with enjoyment.

- The offence of sexually harassing a minor is punishable by a fine and possible imprisonment of up to three years under Section 12 of the Criminal Code.

Section 13: Using child for pornographic purposes and punishment therefore.

According to this section of the law, the perpetrator of the crime of using a child for pornographic purposes is guilty of the offence if they use a child for the purpose of obtaining sexual gratification in any form of media, including advertisements or programmes that are broadcast on television channels, the internet, or any other electronic or printed form. The following are examples of using a youngster for sexual gratification[3]:

- Symbolic representation of a child's developing sexual organs;

- using a kid for the performance of actual or simulated sexual actions (with or without penetration);

[1] https://www.indiacode.nic.in/handle/123456789/2079?sam_handle=123456789/1362

[2] Gautam, Ritu, Cyber crime in India, Availablr at: http://hdl.handle.net/10603/250817

[3] Gautam, Ritu, Cybercrimes and International legal regime, Available at: https://shodhganga.inflibnet.ac.in/bitstream/10603/250817/10/10_chapter-iv%20%20cybercrime%20issues%20and%20international%20legal%20regime.pdf

- The depiction of a kid in a manner that is lewd or offensive.

Punishment under Section 14: the penalty for a first conviction is either a fine or a term of imprisonment that can last up to five years. A jail sentence that can last up to seven years and a fine are the penalties for a second or subsequent conviction.

INITIATIVES OF THE GOVERNMENT

The government has taken a number of steps, including as amending the "Protection of Children from Sexual Offenses (POCSO) Act"[4] in 2019 to add a definition of child pornography under Section 2(da) and providing punishments for violations of Sections 14 and 15 of the Act. In addition to this, both the IPC and the IT Act have been updated to include new provisions for the punishment of cybercrime. In addition, the government has taken a number of measures to combat cybercrime committed against children. These include the creation of specific provisions dealing with cybercrime committed against children, the launch of a web portal and helpline number to file complaints, and the implementation of a variety of safeguarding measures such as the use of filtering software, the monitoring of websites, and the blocking of access to websites containing child pornography. In addition to this, the government has published a variety of instructions to prevent crimes committed online against minors. According to the information provided by the Ministry of Women and Child Development, the government has issued some guidelines, which include the following provisions:

"The provisions of Section 67B of the Information Technology Act of 2000"[5] that deal with cyber crimes committed against minors call for severe penalties for the posting, viewing, or transmission of content in electronic form that depicts children engaging in sexually explicit acts, etc.

Under addition, the "Indian Penal Code, 1860 has provisions for the penalty of online bullying and cyber stalking in sections 354A and 354D"[6] respectively.

"The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021"[7], which were notified under the IT Act, stipulate that intermediaries are required to inform users of computer resources not to host, display, upload, modify, publish, transmit, update, or share any information that is, among other things, obscene, pornographic, paedophilic, harms minors in any way; violates any law that is currently in effect; and so on.

The Central Bureau of Investigation (CBI), which is India's national nodal agency for Interpol, provides the government with INTERPOL's "worst of list,"[8] which the government uses to regularly prohibit websites that include severe "child sexual abuse material (CSAM)"[9].

[4] https://www.indiacode.nic.in/handle/123456789/2079?sam_handle=123456789/1362

[5] https://indiankanoon.org/doc/176300164/

[6] https://www.indiacode.nic.in/show-data?actid=AC_CEN_5_23_00037_186045_1523266765688&orderno=394

[7] https://prsindia.org/billtrack/the-information-technology-intermediary-guidelines-and-digital-media-ethics-code-rules-2021

[8] https://www.interpol.int/en/Crimes/Crimes-against-children/Blocking-and-categorizing-content

[9] Gautam, R., Medical health condition of prisoners and discrepancy in facilities among the states of Uttar Pradesh, Haryana and Delhi, International Journal of Health Sciences Follow journal, DOI: 10.53730/ijhs.v6nS6.12256

Concerned Internet Service Providers (ISPs) have been given an order by the government to come up with an acceptable system for obtaining the Internet Watch Foundation (IWF), UK list of CSAM websites/webpages on a dynamic basis and to ban access to child pornography websites/webpages.

The Department of Telecommunications has requested that all Internet Service Providers (ISPs) make the appropriate arrangements to raise awareness among their subscribers about the use of parental control filters in the end-user machines by sending out messages via email, invoices, SMS, and websites, among other communication channels.

"On August 18, 2017, the Central Board of Secondary Education (CBSE) sent instructions to schools about the usage of the internet in a way that is safe and secure."[10] This circular instructs schools to implement effective security rules and software mechanisms across all of their systems, including effective firewalls, filtering software, and monitoring software.

The government is in the process of putting in place a comprehensive central sector programme that goes by the name "Centre for Cyber Crime Prevention against Women and Children (CCPWC)"[11] to deal with any and all issues concerning the prevention of cybercrime committed against women and children, including child pornography.

The government has established the National Cyber Crime Reporting Portal, which can be accessed at www.cybercrime.gov.in. This portal is designed to allow citizens to file complaints regarding any and all types of cyber crimes, with a particular emphasis on cyber crimes committed against women and children. Complaints submitted through this online system are forwarded to the appropriate state law enforcement authorities for investigation.

In addition, a toll-free hotline number [155260] is now operational across the country to assist members of the public in using the portal to file complaints.

A guide titled "Cyber Safety for Adolescents and Students"[12] has been created by the government in order to educate young people about the many different kinds of online crimes and how they may prevent themselves from falling victim to these kinds of offences. The manual may be accessed on the websites www.mha.gov.in and www.cybercrime.gov.in. The Handbook is also made available to the public by the Ministry of Education on the NCERT website.

The Central Government has taken steps to strengthen the mechanism to deal with cyber crimes in a comprehensive and coordinated manner. These steps include increasing public awareness about cyber crimes, the issuance of alerts and advisories, capacity building and training for law enforcement personnel, prosecutors, and judicial officers, improving cyber forensic facilities, and other similar measures.

[10] https://timesofindia.indiatimes.com/home/education/cbse-issues-cyber-rules-for-schools/articleshow/60125999.cms

[11] https://www.mha.gov.in/division_of_mha/cyber-and-information-security-cis-division/Details-about-CCPWC-Cyber crimePrevention-against-Women-and-Children-Scheme

[12] https://opengovasia.com/indias-initiative-for-cyber-crimes-against-women-and-children/

The Indian government has devised a plan called the "Indian Cyber Crime Coordination Centre (I4C)"[13] in order to take a comprehensive and coordinated approach to dealing with online criminal activity.

CONCLUSION

This research has examined the subject from every angle and has conducted an in-depth examination of the research objectives using a wide variety of primary and secondary sources of information, such as books, journals, various related websites, NCRB data, and discussions with subject matter experts. After conducting research on online crimes committed against children, it has become abundantly clear that online crimes committed against children have skyrocketed by more than 400 percent. Furthermore, it has become evident, after conducting an analysis of the data collected by the NCRB from 2017 to 2020, that instances of child pornography are high in number each year and are exhibiting tremendous growth each year. It has also been observed that these offences are recorded more frequently in metropolitan areas, where there is also a lack of information regarding usages and protective precautions. Despite the fact that the government has released a number of different rules and a site via which people may lodge complaints against it, the reporting rate is still relatively low due to a lack of understanding of the legal and procedural procedures. Based on an examination of the data collected by the NCRB, it seems that the most prevalent types of cybercrimes committed against children during the pandemic include sexual abuse of minors, cybersex trafficking, cyber bullying, child grooming, and other similar offences. As a result of the fact that women and children are among the most defenceless members of society, they were an easy target for perpetrators of cybercrime and sexual predators during the lockdown.

The Indian legal system has enacted a number of different regulations in order to combat the cybercrimes that are committed against women and children. The findings of this research pointed to a few key takeaways for reducing the risk of youngsters being victims of online crime. These include the following:

The first and most important thing for a victim to do is to file a complaint about the cybercrime with the nearest cybercrime cell or on the National Cybercrime Reporting portal. If the victim does not have access to any of these platforms, they can file a FIR with the local police station instead. The provisions of the Information Technology Act of 2000, the Indian Penal Code of 1860, the Indecent Representation of Women (Prohibition) Act of 1986, and the Protection of Children from Sexual Offenses Act of 2012 all prohibit the above-mentioned cybercrimes against women and children and also punish the offender with stringent punishments including imprisonment and fines.

Parents, schools, and teachers all need to keep a close eye on their children as they navigate the internet and use various websites.

They need to be educated about the negative impact that their actions will have on their life, image, reputation, and other aspects of their lives. They should prevent their children from accessing harmful websites by installing parental controls and monitoring software on their children's PCs.

[13] https://www.pib.gov.in/PressReleasePage.aspx?PRID=1814119

The federal government is required, on a regular basis, to ban access to websites that provide severe child sexual abuse material (CSAM), using the "worst of list" compiled by INTERPOL and sent by the Central Bureau of Investigation (CBI).

Internet Service Providers (ISPs) should make suitable arrangements to spread awareness among their subscribers about the use of parental control filters in the end-user machines through messages of email, invoices, SMS, website, etc..Internet Service Providers (ISPs) should make suitable arrangements to spread awareness among their subscribers about the use of parental control filters in the end-user machines.

In addition to putting into place strong security measures, educational institutions are required to implement efficient firewalls, filtering and monitoring software mechanisms in all of the machines.[14]

The victim is required to register a report using one of the many accessible sources, such as the National Cyber Crime Reporting Portal, www.cybercrime.gov.in, or a helpline number that is available nationwide [155260].

Our system of law enforcement should approach the problem of cybercrime in an all-encompassing and well-coordinated manner. This should include activities such as raising public awareness of the issue, issuing warnings and advisories, increasing the capacity of law enforcement personnel, prosecutors, and judicial officers, and improving cyber forensic facilities, among other things.

[14] Gautam, R., "Proliferation of Cyber Crime and Indian legal system with special reference to Gwalior Division" Available at: https://shodhganga.inflibnet.ac.in/handle/10603/250817 Retrieved on: 22/07/2021

11

CYBER CRIMES IN BANKING SECTOR IN INDIA: A CRITICAL ANALYSIS

KEYWORDS

CYBER CRIMES, INDIAN BANKING INDUSTRY, INFORMATION TECHNOLOGY REVOLUTION, INTERNET BANKING

CHAPTER ELEVEN

CYBER CRIMES IN BANKING SECTOR IN INDIA: A CRITICAL ANALYSIS

AUTHOR

DR. RAJU MAJHI, ASSISTANT PROFESSOR, LAW SCHOOL, BANARAS HINDU UNIVERSITY, VARANASI, INDIA

ABSTRACT

As we are well aware that the Indian Banking industry is old and it is very fact that that any changes are brought in this industry since liberalization only. The Indian banking system is well regulated and supervised, it involves moral practice, financial distress and company governance. It is regulated and well supervised by the Central Bank of the country i.e., Reserve Bank of India. It is undeniable fact that with the advancements in technology, the Indian Banking Sector has been at par with the emerging trends and significant changes required in its operations. The rapid growth in technology has given the banking sectors an immense opportunity and as a result, banks are now among the biggest beneficiaries of the Information Technology Revolution. The proliferation in online transactions mounting on technologies like NEFT (National Electronic Fund Transfer). RTGS (Real-Time Gross Settlement), ECS (Electronic Clearing Service) and mobile transactions is a glimpse of the deep-rooted technology in banking and financial matters. The Reserve Bank of India is peeping into the legal compliance of online banking to guarantee monetary dependability. On the other hand, security threats play a predominant role in the Internet banking.

As technology develops, the cybercrimes endanger in the virtual world, people and organizations become the prey at an alarming rate as solely depending on web. Usage of internet and other technologies have enhanced the risk of attacks from cyber criminals across the globe and the banking transactions is also adversely affected. With the sharp rise of cybercrimes, banking sector is the hub in the occurrences of theft, phishing, PC infections, hacking and so on. With these backgrounds this paper aims to examine the technical aspects of various types cyber crimes concerning the banking sectors in India and it also provides certain valuable suggestions to curb down the cyber crimes in banking sectors in India.

INTRODUCTION

Banking plays a vital role in the development of economic systems of any country. Today we cannot imagine the economic prosperity of any nation without the development of banking sector in that country. Economy is one of the pillars which defines the progress and growth of a nation. Banking sector considered as the backbone of the economy. For our day-to-day transactions, we enter into monetary transactions in the form of cash payment, cheques or demand drafts. However, this trend has paved the way to a modern system of payment in the form of swiping of debit cards or credit cards. On the recommendation of the Committee on Financial System (Narasimham Committee) 1991-1998, information and technology in banking sector was used.

The Indian Banking industry is old and many changes are brought in this industry since liberalization. The banking system is well regulated and supervised; it involves moral practice, financial distress and company governance. The call for development has given this unit monstrous probability and so; banks are presently among the best recipients of the Information Technology insurgence. The on-line exchanges mounting on advancements like NEFT (National Electronic Store Exchange), RTGS (Constant Gross Settlement), ECS (Electronic Clearing Administration) and transportable exchanges has provided aid in saving cash and fund problems.

It is very pertinent to see here that on one hand, technology has created advantage for banks and financial institutions but on the other hand, there have been risks involved in it as well. Technology risks not only have a direct impact on a bank as operational risks but can also exacerbate other risks like credit risks and market risks. Given the increasing reliance of customers on electronic delivery channels to conduct transactions, any security related issues have the potential to undermine public confidence in the use of e-banking channels and lead to reputation risks to the banks. Inadequate technology implementation can also induce strategic risk in the terms of strategic decision making based on inaccurate data.

Banking sector has witnessed expansion of its services and strives to provide better customer facility through technology but cybercrime remains an issue. Information which is available online is highly susceptible to be attacked by cyber criminals. Cybercrimes result in huge monetary losses which are incurred not only by the customer but by the banks also which affects economy of a nation. Non-monetary cybercrime occurs when viruses are created and distributed on other computers or confidential business information is posted on Internet. The most common of it is phishing and pharming. Against this background this paper aims to analyse the various problems faced by banking sectors in India by inventing and adopting the e-banking in their systems.

REVIEW OF LITERATURE

To better understand of the subject matter is very necessity to have a look on some of the works which have been done in this regard. This paragraph gives a little overview on some scholars.

RBI, Cybercrime fraud 2019, the total value of bank frauds more than doubled in 2019-2010. Total cases of frauds have increased 159% by value of Rs.1.85 lakh crore, compared to Rs.71.543 crore in 2018-2019. Similarly, the frauds increased 28% by volume to 8707 cases in 2019-2020, compared to 6,799 instances in the previous year, as per data released by Reserve Bank of India in its annual report.

Balasubramanian et at, (2024) analyzed the success of Information System in interest banking and its security challenges. 52 respondents were surveyed customers have fear that information sent by them through internet is not protected also have threat of their bank's website getting hacked. The customers have the fear of the malware attacks. The customers have the doubt about the security system of bearing reliable for internet banking service.

STATEMENT OF THE PROBLEM

It is one of the utmost important areas to analyse or to understand thoroughly it is necessary first to find out the problem. Today, web technology has emerged as an integral and indispensable part of the Indian Banking sector. The enlargement of non-cash-based transactions around the globe has resulted in the steady development of robust online payment system.

The last few years have seen a significant increase in cybercrime across all sectors and geographies. Given the proliferation of this technological crime, organizations face a significant challenge to be resistant against cyber-attacks. Digital India may have become a soft target for criminals as country recorded a huge increase of 63.5 percent in cyber-crime cases in the year 2019, showed the National Crime Record Bureau data. The NCRB's data stated that 44,546 cased of cyber-crimes were registered in 2019 as compared to 28,248 in 2018.

This research attempts to analyses the concerns of cybercrimes in e-banking sector by highlighting the various wrongdoings are reported on a regular basis in the Indian Banking Sector. There is a need to analyses the nature of such crimes so that appropriate preventive measures may be devised.

OBJECTIVES OF THE STUDY

As far as concerned to the objectives of the study, there are two very significant objectives have set out to examine the problems thoroughly. These are:

1. To identify the various cybercrimes in e-banking sector in India.
2. To provide the preventive measures to control the cybercrimes in India.

RESEARCH DESIGN

Research design is an integral part of any research work. To complete this research paper the focus of the study has been on describing the various cybercrimes and the preventive measure to overcome these issues. The research design chosen for the study has been descriptive and the secondary data source has been collected through web-sites, books and journals. The period of the study was tall till February 2022.

LIMITATIONS OF THE STUDY

Any work is not absolutely complete itself; this work has also its limitation. This study focuses on the cybercrimes related only to the Indian e-banking sector. It does not cover the whole financial sector. All aspects area and measures covered are limited to the Mobile and Internet Banking users.

After describing the framework of the research work, now it very significant to have a brief looks on the concept of e-banking.

CONCEPT OF E-BANKING

It is very general term now days used in the banking sector to complete any banking transactions i.e., Electronic Banking or e-banking. Electronic Banking or e-banking refers to a system where banking activities are carried out using informational and computer technology over human resources. In comparison to traditional banking services, in e-banking there is no physical interaction between the bank and the customers. e-banking is the delivery of bank's information and services by banks to customers via different delivery platforms that can be used with different terminal devices such as personal computer and a mobile phone with browser or desktop software, telephone or digital television. The first initiative in the area of bank computerization was stemmed out of two successive Committees on Computerization (Rangarajan Committee). The first committee was set up in 1984 which drew the blueprint for the mechanization and computerization in Banking Industry. The second Committee was set up in 1989 which paved the way for integrated use of telecommunications and computers for applying fully the technological breakthroughs to the banking operations. The focus shifted from the use of Advanced Ledger posting Machines (ALPMs) for limited computerization to full computerization at branches and to integration of the branches. Till 1989, banks in India had 4776 ALPMs at the branch level, over 2000 programmers/systems personnel and over 12000 Data Entry Terminal Operators. e-banking is also known as Cyber Banking, Home Banking and Virtual Banking. e-banking incudes Internet Banking, Mobile Banking, RTGS, ATMs, Credit Cards, Debit Cards, and Smart Cards tec. Some of the forms of e-banking are explained below:

(1) *Automated Teller Machines (ATMs)*

An ATM is a device which is located on or off the bank's premises. It enables a customer to withdraw cash, obtain statement of law few transactions in his/her account, deposit cash and to transfer funds from one account to another. A person can withdraw cash 24x7 from ATMs subject to the limit provided. This system is also known as "Any Time Money" or "Anywhere Money". To have access of ATM a person must have an ATM card. The ATM card is inserted into the machine and the client is required to enter a personal identification number (PIN). PIN is the numeric password which is separately mailed or handed over or sent by post to the customer by the bank while issuing the card. Most of the banks require that customers change their PIN after first use. Banks also sends alerts to the customers not to disclose their PIN to anybody, including to bank officials. Customers should change the PIN at regular intervals. The transactions carried out using ATM machines are quite easy. There are two types of ATMs, one, exterior ATMs which are located in shopping centers, railway stations, airports etc, and second, interior ATMs which are located within the bank premises. The limits on cash withdrawal at ATMs and for purchase of goods and services are decided by the issuer bank. Nowadays a customer can use ATM of another bank also to withdraw cash. However, in case of such withdrawal at other bank's ATM, there is a limit of cash withdrawal.

(2) *Real Time Gross Settlement System (RTGS)*

RTGS is a system where funds are transferred from one bank to another on "real time" and "gross basis". RTGS transactions are carried through either interbank or it can be between customers through bank accounts. "Real Time" means the processing of instructions at the time they are received rather than at some later time; 'Gross Settlement' means the settlement of funds transfer instructions occurs individually (on an instruction by instruction basis). The transactions are settled individually in RTGS. RTGS transactions are processed throughout the business hours of banks. The timings of business hours at different bank branches are decided by the banks on their own terms and policies. Generally RTGS transactions for customers are available from 9:00 hours to 16:00 hours on weekdays and from 9:00 to 14:00 hours on Saturdays where settlement is to be done at the Reserve Bank of India end. In the RTGS system, mainly large value transactions are processed. The minimum amount that can be remitted through RTGS is Rs. 2 Lakhs. Only minimum limit is provided for payment transaction through Reserve Bank of India settlement. No maximum limit is prescribed for RTGS transactions. Credit card and Debit Card Banks issue debit cards that are linked to a customer's bank account. Debit Cards can be used to transfer funds only for domestic purposes from one person to another person. At present, a customer can use his Debit Card to withdraw money, known the monthly statement etc., by using another bank's ATM, not being the ATM of the bank, which issued such debit card. In case a customer transacts through an ATM of another bank from his savings bank account using his debit card then he is not charged by his/her bank up to five transactions which includes both nonfinancial and financial transactions in a month. However, these five free transaction limits for transactions done at ATM of another bank is restricted to three transactions in six metro cities which incudes, Delhi, Mumbai, Chennai, Bengaluru, Kolkata and Hyderabad. Like Debit cards, it is the banks/another entity permitted by Reserve Bank of India who use credit cards to a customer. A Credit Card has dimension of about 8.5 cm by 5.5 cm. It is a small rectangular shape plastic card bearing the name of the holder of the card i.e., the customer and the account number is printed over it. In addition, the date up to which the card is valid will also be embossed and a specimen signature panel on the revere. A card holder is also given the list of shops and establishments in each city where the card will be accepted in lieu of cash. The limit up to which the card holder can make purchases in a month is also informed to the card holder, this limit is called card limit.

(3) *Internet Banking in India*

Internet Banking is a result of computerization of banking sector. it was necessary for the banks to open up internet banking activities because of cut-throat competition. Furthermore, Internet banking facility being available at all time has created an advantage for the customers. There has been a paradigm shift from "bricks and Mortar" to "click and mortar" in the banking sector. The first bank to start with internet banking facility was ICICI followed by IndusInd Bank and HDFC Ban respectively in 1999. Internet Banking is beneficial because it is convenient and easy to do banking business from home or at office desk. One can avoid standing in long queues or delays. Simply by logging using User ID and Password one can experience Internet Banking. With a click on the internet, a customer can check his account statement, transfer funds from one account to another, open FD (fixed deposit), pay electricity or telephone bills or pay rent, can recharge his/her postpaid or prepaid bills etc. Electronic keeping money or e-managing an account alludes where saving money exercises are completely utilizing instructive and Personal Computer innovation over human asset. In contrast to the traditional method in e-managing there is no physical association with the banks and their customers.

E-managing is the conveyance of banks data and administration to clients by means of various conveyance stages which can be utilized through Personal Computer and Mobile Phones or advance Television.[1]

A working gathering on managing was established by the Reserve Bank of Indi. For the management and administration, the gatherings portioned money into 3 categories:

(a) Enlightening Framework: This category gives data about credit plans, branch areas, financing costs to the clients. The client can download different utilities according to their personal needs. There is no sensible possibility of any unapproved individual getting into the creation arrangement of the bank.[2]

(b) Open Framework: This gives data to client about his record balance. The data can be checked by clients after confirmation and signing through passwords.[3]

(c) Value Based Framework: In this category the clients can do changes through its framework and they are directly transferred to the clients record. A bi-directional change takes place between the bank and client and between client and the outsider. This framework is used through instruments like http and https. E-keeping money incorporates Web Saving money, Portable Managing an account, RTGS,

[1] Daniel, E (1999), Provision of electronic banking in the UK and Republic of Ireland, International Journal of Book Marketing, Vol.17 No.2.

[2] Reserve Bank of India, Report on Internet Banking. available at : https://www.rbi.org.in/Scripts/PublictionReportDetain.aspx?UrlPage=&ID=243#ch2(Last visited: February 27,2022 at 17:00 Hrs.)

[3] *Ibid.*,

ATMs, Master Cards, Charge Cards and keen cards and so forth.[4]

(4) *Mobile Banking*

The importance of mobile phones for providing banking services has increased. We have become dependent on our mobile phones these days. Because of the growth of mobile phone subscribers in India, banking services have been extended for the customers to be availed through their mobile phones. Mobile banking is when transactions are carried out using a mobile phone by the customers that involve credit or debit to their accounts. In 2014, the Reserve Bank of India had set up a Committee on Mobile Banking under the Chairmanship of B. Sambamurthy. The Committee is required to study the problems faced by the banks in providing mobile banking to the customers and to examine the options including the feasibility using encrypted SMS-based funds transfer. Mobile banking facility has witnessed tremendous growth in our country. In the financial year (2016-2017), mobile wallets overtook mobile banking in number of transactions. Mobile wallets transactions; from phone recharges to paying for cabs or shopping online; trebled to almost 400 million through April-November 2016. Mobile wallet system is there in Apps like Jugnoo, Ola, Uber, Mobikwik, Paytm etc.

MEANING OF THE TERM CYBERCRIME

Until mid-1990s, managing an account segment in many parts of the world was basic and dependable; anyway since the coming of innovation, the keeping money division saw a change in perspective in the wonder. Banks so as to upgrade their client base presented numerous stages through which exchanges should be possible absent much exertion. These advancements empowered the client to get to their banks funds 24x7 and year around through, ATMs and Web based managing an account methods.

With the pace in innovation, the money cheating cases have increased. Cyber criminals are using different techniques to collect bank data and last their cash. Various specialized techniques have been used by the banks to safeguard these crimes, but this issue still holds on. The explanation for this is the resistance measures right now accessible with banks are accessible in the open market or area which can be used by a digital criminal, who can easily cross the safety standards. One of the techniques to relieve the issue of digital wrongdoings in keeping money segment is to distinguish the variables by banks and the issue of digital wrongdoings. Banks which is the most part focuses of digital wrongdoings experience the ill effects of different online assaults like phishing, keystroke, logging malwares, wholesale fraud etc.

CYBERCRIME IS BANKING SECTOR

Digital wrongdoing can be explained as a contravention that includes places of wrongdoing, target, instrument source, Personal Computer and a network as a medium. With the increased digital based business transactions,

[4] Dheenadhayalan V. Automation of Banking Sector in India, Yojana, February (2010) p.32.

these wrongdoings have floated towards an advanced world.[5]

These kind of digital assaults are increasing all around India has been seeing a sharp increase in digital contravention cases in a previous few years. In 2016 an investigation by Juniper Exploration evaluated that worldwide expenses of cybercrime could be as high as 2.1 trillion by 2019.[6]

Digital violations can be comprehensively be arranged into classification such as digital harassing, programming robbery, wholesale fraud, e-mail spam, online robbery.

In general cybercrime may be defined as "Any unlawful act where computer or communication device or computer network is used to commit or facilitate the commission of crime"

However, from the aspect for financial cybercrimes committed electronically, the following categories are predominant:

(1) **Hacking:** It is a technique to gain illegal access to a computer or network in order to steal, corrupt, or illegitimately view data.

(2) **Phishing:** It is a technique to obtain confidential information such as usernames, passwords, and debit/credit card details, by impersonating as a trustworthy entity in an electronic communication and replay and same details for malicious reasons.

(3) **Vishing:** It is the criminal practice of using social engineering over the telephone system to gain access to private personal and financial information from the public for the purpose of financial reward.

(4) **Spamming:** Unwanted and unsolicited e-mails usually sent in bulk in an attempt to force the message on people who would not otherwise choose to receive it are referred to as Spam e-mail.

(5) **Denial of Service**: This attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service by "flooding" a network to disallow legitimate network traffic, disrupt connections between two machines to prohibit access to a service or prevent a particular individual from accessing a service.

(6) **ATM Skimming and Point of Sale Crimes**: It is a technique of compromising the ATM machine or POS systems by installing a skimming device atop the machine keypad to appear as a genuine keypad or a device made to be affixed to the card reader to look like a part of the machine. Additionally, malware that steals credit card data directly can also be installed on these devices. Successful implementation of skimmers cause in ATM machine to collect card numbers and personal identification number (PIN) codes that later replicated to carry out fraudulent transactions.

(7) **Virus, Worms and Trojans:** Computer Virus is a program written to enter your computer and damage/alter your files/date and replicate them. Worms is malicious programs that make copies of themselves again and again on the local drive, network shares, etc. A Trojan horse is not a virus. It is a destructive program that looks as a genuine application. Unlike viruses, Trojan horses do not replicate themselves but they can be just as destructive. Trojans open a backdoor entry to your

[5] Kharouni, L (2002) Automating Online Banking Fraud Automatic Transfer System: The Latest Cybercrime Tookkit.

[6] Liu, J., Hebenton B & Jou, S Handbook of Asian Criminology.

computer which gives malicious users/programs access to your system, allowing confidential and personal information to be theft.

REASONS FOR CYBERCRIME

Ha a very brief looks on reasons of cybercrimes. In this regard it very relevant to put forward the observation of Hart. Hart in his work, the idea of law has said people are helpless so standard of law is required to ensure them. After applying this may state that Personal Computers are powerless so standard of law is required to secure and protect them against digital wrongdoing. Following are some reasons.

1. Loss of Proof
2. Negligence
3. Complex
4. Easy to access
5. Capacity to store information in little place.

IMPACT OF CYBERCRIME ON BANKING SECTOR

It is very important to analyse the impact of cybercrimes on Banking Sector in India. As above it is already mentioned that the economic system of any nations is very important for the prosperity of the banking sector which leads nation's prosperity. In this context we have to see the main cases have been identified because of the violent upsurge in cell phones with internet. Mobile phones are used for a number of online services like web saving money, paying service changes; web based shopping and is according to the criminals to acquire access to criminal data.

In the cases, where the hackers are not able to get significant data, destroy of the bank's site as a measure to render against their endeavors.

Other than monetary benefits from digital assaults, the illicit business generally termed as the Darkweb,[7] adds to the cybercrime, as a tool for trading individual data. Touchy data including stolen Card Numbers web-based managing account, therapeutic records and authoritative access to servers are exchanged for cash in this online network.

After discussing all these issues, it is very pertinent to see that what kind of legal systems or laws are prevailing in India to eradicate the problems of cybercrimes on banking sector in India. The next paragraph an attempt has been made to analyse the existing laws in India to curb the cybercrimes in banking sector in India.

[7] Murashbekov, OB. (2015), Methods for Cybercrime Fighting Improvement in Developed Countries, Journal of Internet Banking and Commerce.

LEGAL REMEDY AVAILABLE FOR CYBER TERRORISM UNDER INFORMATION TECHNOLOGY ACT, 2000

In absence of a proper and strong legal system, the crime or criminals cannot be control. To control and give an effective solution to these problems, we must have a very effective and appropriate law. The threat created by the malware for cyber terrorism is successfully controlled provided that provisions of the Indian Penal Code with the strict provision of the data Technology Act, 2000 jointly implemented. Courts can use their discretion by combining provisions of assorted statutes to try and do the entire justice goodbye the provisions of Information Technology Act, is added on with the provisions of Indian Penal Coded to manage the cyber terrorism. The protection of Information Technology Act is claimed for:

Violations of Privacy: Right to privacy could be part of the proper to life and private liberty enshrined under Article 21 of the Constitution of India. The assorted provisions of the Information Technology Act, 2000 pertinently protect the web privacy rights of the citizens. The legal remedy available against the culprit using the malware, Section 1(2) read with Section 75 of the Information Technology Act, 2000 provides for an extra-territorial application of the provisions of the Act. Thus, if someone (including a far off national) contravenes the privacy of a personal by means of computer, system or network located in India, he would be liable under the provisions of the Information Technology Act, 2000.

Prevention of data and data theft: Provisions of Information Technology Act, 2000 handling the information under Section 43, Section 65, Section 66, Section 70 and Section 72 may be successfully invoked. Likewise Provisions of Information Technology (Amendment) Act, 2008 under Section 43A and Section 72A jointly supplemented with Section 22 of Indian Penal Code, 1860 and 378 of Indian Penal Code will be invoked.

Prevention of distributed denial of services attack: A malware can also use the strategy of distributed denial of services (DDOS) to overburden the electronic bases of people. Thus, distribute denial of services by use of malware are going to be tackled by invoking the provisions of Section 43, Section 65 and Section 66 of the Information Technology Act, 2000 collectively.

Prevention of network damage and destruction: In India there is no law, which is specifically coping with prevention of malware through aggressive defense. Thus, the analogous provisions must be applied in an exceedingly purposive manner.

CONCLUSION

Against this background this paper is concluded by providing some of the precautions, which may help to minimize the cybercrimes. The present conceptual framework has provided a bird's eye view of ongoing efforts to prevent and control highly technological and computer based crimes, and highlighting general trends and developments within and without the Indian Banking Sector. This study has described deeply a number of common electronic crimes, identified in the specific areas of Indian Banking Sector. The study has provided an overview to the concept of e-banking by discussing deeply various cyber-crimes, identified specifically in the banking sector. The Banking system is the lifeblood and backbone of the economy,

Information Technology has become the backbone of the banking system. It provides tremendous support to the ever increasing challenges and banking requirements. Presently, banks cannot think of introducing financial product without the presence of Information Technology. However, Information Technology has had an adverse impact too on our banking sector where crimes like, phishing, hacking, forgery, cheating etc., are committed. There is a necessity to prevent cybercrimes by ensuring authentication, identification and verification techniques when a person enters into any kind of banking transaction in electronic medium. The growth in cybercrimes and complexity of its investigation procedure requires appropriate measures to be adopted. It is imperative to increase the cooperation between the stakeholders to tackle cybercrimes. According to National Crime Records Bureau, it is found that there has been a huge increase in the number of cybercrimes in India in past three years. Electronic crimes are a serious problem. In cases of cybercrimes, there is not only financial loss to the banks but the faith of the customers upon banks is also undermined. Indian banking sector cannot avoid banking activities carried out through electronic medium as the study suggest that there has been an increase in the number of payments in e-banking. However, the change in the banking industry must be such the suits the Indian market. Banks are required to be updated and ahead with the latest developments in the Information Technology Act, 2000 and the rules, regulations, notifications and order issued therein pertaining to bank transactions and emerging legal standards on digital signature, electronic signature, data protection, cheque truncation, electronic fund transfer etc., as part of overall operational risk management process. It is the need of the hour to increase cooperation between the countries, over the tools and techniques, which will help them effectively to counter global electronic crime. In developing countries, like India, cyber and electronic crime poses a serious problem because there is a lack of training on the subjects related to investigation of electronic and cybercrimes. Lastly, it can be concluded that to eliminate and eradicate cybercrimes from the cyberspace is not a seemingly possible task but it is possible to have a regular check on banking activities and transactions. The only propitious step is to create awareness amongst people about their rights and duties and to further making the implementation of the laws more firm and stringent to check crime.

At the end of this paper some for very import precaution measures are incorporated in practice while making e-banking transactions, which may some extent, help to minimize the incidents of cybercrimes. There are some very important preventive measures have suggested which from time to time Reserve Bank of India and banking sectors have been issued under their guideline to prevent the cybercrimes. These may be summed as follows:

1. Always keep your systems/devices (desktop, laptop, mobile) updated with latest patches and Protect systems/devices through security software such as anti-virus with the latest version.
2. Ensure all devices/accounts are protected by a strong PIN or pass code. Never share the PIN or password with anyone.
3. Computers/laptops should have a firewall and antivirus installed, enabled and updated with latest versions. Never download or install pirated software, applications etc., on your computer, laptops or hand-

held devices. Always scan external devices for viruses, while connecting to the computer.

4. Ensure all devices/accounts are protected by a strong PIN or pass code. Never share your PIN or passwords with anyone.
5. Do not share your net-banking passwords. One Time Passwords (OTP), ATM or phone banking PIN, CVV number etc., with any person even if he/she claims to be an employee or a representative or the bank and report such instances to your bank.

12

IMPACT OF CYBERCRIME ON CHILDREN & ADOLESCENTS

KEYWORDS

CYBERCRIME, HARASSMENT, SEXUAL ABUSE, PORNOGRAPHY, CYBER STALKING

CHAPTER TWELVE

IMPACT OF CYBERCRIME ON CHILDREN & ADOLESCENTS

AUTHORS

DR. SUSHMA SINGH, ASSISTANT PROFESSOR, SCHOOL OF LAW, SHARDA UNIVERSITY, GREATER NOIDA, UTTAR PRADESH, INDIA

SHAFIA NAZIR SHAH, RESEARCH SCHOLAR, SCHOOL OF LAW, SHARDA UNIVERSITY, GREATER NOIDA, UTTAR PRADESH, INDIA

ABSTRACT

The term “cybercrime,” which refers to an offence committed via the internet, is well-known around the world. When it comes to cyber security, it’s the newest and most complex issue. A computer is either the tool or the target of a cybercrime. People throughout the world may now easily access information and data thanks to the internet’s development. Although the internet has many advantages, some people abuse computers and the internet for criminal purposes, such as online pornography, cyber stalking, spamming, viruses, and hijacking web pages. Offenders also utilise the internet as a platform for child abuse, which is a type of cybercrime. Child sexual exploitation is a common kind of violence against children and adolescents in cyberspace and they are the most recent victims of cybercrime. Criminals prey on youngsters by engaging them in illicit practises such as online grooming, the production, distribution, and possession of child pornography, exposure to hazardous content, harassment, and sexual abuse, cy-

ber bullying etc. Today, cybercrime is becoming a global issue of considerable concern. The pace of technological advancement in India is accelerating due to the COVID-19 pandemic, children have been spending more time on virtual platforms, which has exposed them to online harassment and cyber bullying. However, not all youngsters are equipped with the information and resources to protect themselves online. According to the NCRB 2020 data, the number of incidents of cybercrime targeting children has increased dramatically since last year. In 2019, there were 164 reports of cyber crimes against children, compared to 117 in 2018, and 79 in 2017, all of which were investigated.

INTRODUCTION

All over the world, the term "cybercrime" is used to describe a crime committed via the internet. All over the world, cybercrime is becoming a major topic of discussion. In India, the pace of technological advancement is accelerating. Cybercrimes, including crimes against children, are on the rise as the internet expands and more Indians join the online community. National Crime Records Bureau (NCRB) data shows that cybercrimes against Indian children increased dramatically in 2020 when compared with data from the preceding year.[1] Data from 2020 from the NCRB shows that Uttar Pradesh had the highest number of online offences involving minors (170), followed by Karnataka (144), Maharashtra (137), Kerala (107) and Odisha (108). (71).

Everyone's preferred method of communication is now email, websites, and other web-based tools. It facilitates the exchange and distribution of data, images, and other types of material. It's a good resource, but it also contains some bad information. All of this stems from new information technology inventions that, in order to open up new economic and social opportunities, pose challenges to our security and privacy. In today's world, we're all connected to the Internet. The smart digital gadgets are used by everyone. As part of the "internet of things," all of society's institutions are now interconnected. We're living in a better time because of all the advances made possible by modern technology. Automation is taking hold of the framework. The two most difficult issues to overcome are those relating to personal safety and privacy. Attacks can be used to disrupt services and establish illegal connections. Many of the children's activities are taking place on social networking sites such as playing games, chatting with friends, creating groups, video conferencing, making tik toks, and so forth. Children and adults alike misuse technology for illegal purposes and to express their feelings, conduct themselves in a manner that harasses, threatens, stalks, or damages others, as well as for their own personal gain.

Only a small percentage of school-age children are aware of the many privacy settings available to them on social media. As their personal information is made public, they open themselves up to all kinds of cyberattacks. Today's advancements in internet technology have both positive and negative effects on society, including an increase in crime that targets children in particular. In cases where children are the victims of cybercrime, the perpetrators should be held to account. This includes the use of computers in cyber terrorism: hacking, spamming and viruses; spamming; viruses; credit card fraud; trafficking in pornography; posting of obscene photographs; sending fake e-mails; misuse of personal information; digital piracy; money laundering; counter-

[1] https://www.hindustantimes.com/india-news/,last visited on 16th February 2022.

feiting. By stealing personal information and manipulating data for profit or political gain, these attacks violate privacy. Criminals who pose as victims in online chat rooms and encourage their victims to meet them face-to-face can facilitate child abuse and exploitation, including trafficking and sex tourism. When a child is chatting on the phone, they have no idea who they are talking to. They don't realise they've made a mistake until they actually meet the person with whom they were conversing, who may be an elderly man in his 40s or 50s. A large number of children take their own lives after their obscene images are widely shared on social media sites. Fear or a threat may cause children to keep this from their parents or caregivers, resulting in even more stress and harassment.[2]

In India there is an increase in Cyber Crime:

1. The incidents of cybercrimes rose by almost five times during the year 2011- 2016, as per report by AASSOCHAM.

2. In 2014, cybercrimes grew by 69% vis-à-vis 2013. Similarly, the year 2015 registered an increase of 20.5% in cyber-crimes as compared to the year 2014.

3. Cybercrimes in India almost doubled in 2017, according to statistics released by the National Crime Records Bureau (NCRB) on Oct 22, 2019. In a report published online.[3]

Cyber-attacks can be prevented at the outset if a large number of cyber threats and their impact are understood, as well as a thorough understanding of how they work. The term 'Child' is not defined in the Indian constitution. According to Article 1 of the United Nations Convention on the Rights of the child 1989, "*a child means every human being below the age of eighteen years unless, under the law applicable to the child, majority is attained earlier.*"[4]

As defined by the United Nations for analytical purposes, "youth" is defined as people aged 15 to 24 years without regard to other definitions by member states, and as a result, nearly 27.5% of Indians are between the ages of 15 and 29. Online risks such as addiction and cyberbullying can also have a negative impact on young people, according to new research. It's important to keep in mind that not all children have access to computers or other electronic devices. One of the simplest ways to describe youth is to use their age group, but more research is needed to identify the most at-risk youth and to develop effective interventions.

A 53.5 percent increase in Cyber Crime has been observed over the last few years. According to one report, a large number of cyber criminals, the majority of whom were young adults, were apprehended. Three hundred and twenty-four of those detained under the Information Technology Act of 2015 were between the ages of 18 and 30 years old. Easy money is a major factor contributing to rising crime rates among young people. It is

[2] https://www.indialegallive.com/, last visited on 16th February 2022.

[3] https://www.indialegallive.com/cyber-crimes-and-its-impact-on-children-and-the-alternative-solutions/#google_vignette, last visited on 17th February 20222.

[4] http://www.ohchr.org/EN/ProfessionalInterest/Pages/CRC.aspx, last visited on 17th February 2022.

because of today's youth's selfish and attention-seeking behaviour that they commit heinous crimes. Young and well-educated teenagers are among the most disturbing facts to emerge from the crime reports.

The rate of youth crime has risen to 40%, and nearly 56% of the crimes are committed by those ages 16-25. The traceable young and the reasons aren't obvious, but they play a major role in the alarming numbers:

- First, it's easy to make money.
- Unemployment is a second factor.
- The ability to fit in with others.
- A desire to be noticed.

But blaming the youth for all of it will clearly be wrong. Youth, at most times, in such cases are themselves victims. Many qualified young criminals are drawn to committing crimes due to scarcity of jobs. Also, peer pressure plays a negative role, which leads teenagers to earn money in easy ways, show-off and try to gain attention by buying expensive gadgets.

CYBER CRIMES AND SOCIAL NETWORKING SITES

Rather, the emphasis is on social media users who can keep an eye out for signs of high tension and investigate them if deviations from the 'norm' are detected (level of low tension). There are a variety of ways to represent the "terrestrial" and the "cyber" streets using indicators about community crime, insufficiency, and population analysis. When it comes down to it, the term "neighbourhood infirmities" allows for the official foundations of civil unrest through reference to user generated social media content and its connection to other socially and commercially custodial data. Scholars say that spending time on social media networks is a common pastime among today's children and teenagers. There are a variety of entertainment options for young people, including gaming sites, virtual worlds, and video sites like YouTube. In recent years, this had grown significantly. Parents must be aware of the social media environment because not all of them are safe for children and teenagers.

CYBERCRIME AND THE EFFECTS ON CHILDREN

Many studies have shown that policies and plans for educating young people and individuals about how to protect themselves online can be made more and more effective. Those under the age of 18 should exercise caution when interacting with strangers on the Internet, and they should never give out any personal information. Increasing public awareness of teens' online activities and practises will be made possible through additional research into how they access social networking websites and the false actions they take. As a result of this perspective, better online safety measures and strategies can be devised to keep teenagers safe. It was found that cybercrime has become a major problem in the last two decades. Cyber criminals prefer to prey on today's young adults. Aside from being a victim of a cybercrime, other factors include gender, education, financial status, and even forced victimisation. Females were protected from cyber-bullying through the use of offline social networks. The future harassment was more likely to disturb the young Cyber Crimes games. To make better-quality Tik tok videos, a call centre employee fled with an iPhone, police say, and was arrested at a vehicle check at Vikas Marg, according to the police. An online ad for the sale of an iPhone had been posted by the complainant. An interested buyer called and asked him to meet him at the Preet Vihar Traffic Signal, so he agreed to go. After arriving at the location, the respondent took the complainant's phone and ran off with it. Is there a specific reason why some young people commit cybercrime? Young cyber criminals, it seems, aren't always looking for financial gain when they join the "dark side," as we've all come to expect from cyber criminals. For instance: A report by the National Crime Agency (NCA) in the United Kingdom found that many criminals aren't motivated solely by money. Perceptions from their peers, the popularity of the forums they belong to, and a sense of success are the most important factors in determining their success. According to those who engage in cybercrime, "completing a challenge and justifying oneself to peers are the primary motivations." The testimony of an 18-year-old who was arrested for unauthorised access to a government website is included in this report. "I did it to impress the people in the hacking community, to show them I had the skills to pull it off," he said at the time of his arrest of the child. "I needed to establish my worth."

ROLE OF PARENTS IN CYBERCRIME

It is not just parents and teachers that have to worry about cybercrime, but entire educational institutions. In this virtual environment, it's nearly impossible to avoid being a part of it. However, we may believe that Cyber Crimes do not have a significant impact on the social landscape. Cyber criminals have found a new way to disseminate their crimes thanks to the unstoppable spread of social media. As a result, social media platforms such as Facebook and Twitter are employing a corrupted Cyber Crimes detection process, as well as enlisting the help of a legal expert from the Social Law Network. At an early age, many youngsters have been exposed to the digital world They know a lot more about social media and how to handle it, as well as how to use an app's UI and apply technology to common problems. Like any children, today's youth enjoys experimenting and discovering new things. There is no fear in tweeting, Facebooking, Instagramming, and Snapchatting about your life's most intimate details, according to today's generation. On other people's webpages, they're more prone to post sarcastic or rude remarks. They frequently sign up for phoney online groups and forums, engage in chats with random people, post images of themselves online, and put their personal information at risk by typing it into their smartphones, tablets, laptops, and other electronic devices. They become easy targets for cyber criminals, and they put their family and loved ones at risk as a result of their online activities.

LAWS RELATED TO ONLINE OFFENCES AGAINST CHILDREN

Online offences against children are covered by Several pieces of legislation

i. Protecting children from sexual offences (POCSO) Act, 2012 is a vital piece of law that explicitly handles sexual offences perpetrated against minors. Child pornography, cyber bullying, defamation, grooming, hacking and identity theft are all criminalised by POCSO. POCSO also criminalises online child trafficking, sexual harassment and violation of privacy.

ii. The principal statute in India dealing with cybercrimes against children and adults is the Information Technology Act, 2000. The different rules that have been framed under it serve to supplement it.

iii. Protecting everyone, particularly children, from all offences is the goal of the India Penal Code (1860). Theft, deceit, forgery, mischief, and defamation are only a few of the classic offences that the IPC includes as examples of cybercrime. In some situations, the applicable provisions of the IPC, POCSO, and the IT Act overlap, and an accused may be charged with a number of offences. Anyone found guilty under one, two, or all three acts is sentenced to the most severe penalty.

CONCLUSION & SUGGESTIONS

Despite the fact that not everyone is a victim of Cyber Crimes, they are nevertheless vulnerable. In order to keep themselves safe from internet stalkers, people should keep their personal information private. When it comes to sharing your personal information online, this is as risky as handing out your personal information to strangers in a public place. Always keep an eye on the websites your children are visiting to make sure they aren't being harassed. Leaving cookies unprotected could be fatal, so it's best to use a security application that gives you control over the cookies and sends all the information back to the site.

Here are some strategies to Protect your Child from Cyber Crimes.

i. Cyber Crimes exist, and your child is the most susceptible. Don't let your child's overconfidence fool you into thinking nothing bad will happen to him. Data hackers and virus professionals can get their hands on any information that is provided online.

ii. Report all forms of cybercrime, no matter how minor the offence may seem. If your child has been the victim of Cyber Bullying, for example, you should immediately notify the police because cyber bullies play on people's anxieties and weaknesses to ensure that their crime is not reported. Your vigilance and inventiveness can aid in the capture of some of the most notorious online criminals.

iii. Your child should be taught not to browse and share on sites with a poor track record.

iv. Make sure your child is aware of cyber-crime. Students don't fully grasp the scope of cybercrime as long as most of them are aware of the issue. It is imperative that you discuss the dangers of cybercrime with your child on a regular basis as a parent. Make them aware of the scenarios in which they are vulnerable to criminal activity.

v. Keep an eye on your child's whereabouts at all times. Look for clues to what your youngster has been doing online without invading their privacy. In the event of a difficulty, your child needs to feel safe enough to open up to you.

13

THE FUNCTION OF ARTIFICIAL INTELLIGENCE IN IMPROVING CRIMINAL JUSTICE SYSTEM WITH REFERENCE TO INDIA

KEYWORDS

ARTIFICIAL INTELLIGENCE, CYBER-ATTACKS, CRIMINAL JUSTICE, MACHINE

CHAPTER THIRTEEN

THE FUNCTION OF ARTIFICIAL INTELLIGENCE IN IMPROVING CRIMINAL JUSTICE SYSTEM WITH REFERENCE TO INDIA

AUTHORS

KM. RICHA, RESEARCH SCHOLAR, SCHOOL OF LAW, SHARDA UNIVERSITY, GREATER NOIDA, UTTAR PRADESH, INDIA

DR. SUSHMA SINGH, ASSISTANT PROFESSOR, SCHOOL OF LAW, SHARDA UNIVERSITY, GREATER NOIDA, UTTAR PRADESH, INDIA

ABSTRACT

When Chief Justice of India S.A. Bobde backed the use of artificial intelligence (AI) to address the judicial system's endemic delays, he made an exciting proposal. He believes AI can assist streamline the case load at courts, given the rising number of pending cases and vacancies in the judicial system. It will allow courts to prioritise big, convoluted cases that demand more human attention above simple, routine trials. Cyber-attacks are becoming more common, wreaking havoc on the criminal justice system. Understanding and combating the motive of crime is a critical challenge for law enforcement authorities. The goal of

this study is to show how Artificial Intelligence and Machine Learning, as well as Predictive Analysis with soft evidence, may be used to sort out existing criminal records using metadata, and so forecast crime. Furthermore, it would undoubtedly assist police and intelligence agencies in intelligently investigating crimes by referring to the database, so assisting society in reducing crime through faster and more effective investigation processes. It would also let the analyst follow the activities and connections of various criminal elements based on their most current activities by extracting specific facts from documents or records. This research can be used to understand crime prediction. The current analysis displays the level of threat accuracy from 28 Indian states. When proper data is provided to this model, the chances of prediction are better and more accurate, according to study on the subject. The study also sought to learn more about the psychosocial aspects of crime and what motivates people to commit such crimes.

INTRODUCTION

The design, development, and deployment of artificial intelligence have been the subject of much debate during the last decade (AI). In India, for example, the NITI Aayog recently released an approach paper on the need to use AI responsibly and ethically. The Indian judiciary, which has already put in place basic information and communication technology infrastructure through the e-Courts Project, is now trying to take advantage of AI's potential. The Supreme Court's AI committee has already launched and tested a neural translation tool (SUVAAS) and, more recently, a court administration tool in the last two years (SUPACE). As a result, it's evident that talking about incorporating AI into the legal system isn't a far-fetched idea for decades down the road. In reality, Artificial Intelligence (AI) was initially introduced in Dartmouth in 1956 by its father, John McCarthy. Because technology is the initial layer, digital transformation entails dangers. AI and machine learning (ML) technologies have steadily improved in capabilities and accessibility in recent years, with no signs of slowing down. Understanding the AI rule for the future, its benefits and drawbacks, can make AI beneficial. AI research and regulation aim to strike a balance between innovation's societal security and possible harms and roadblocks. The Indian government is focusing on AI development, adoption, and marketing in order to make society's lives easier. The accuracy and verisimilitude of the specifics regarding where the crimes take place, as well as information on how the crimes are depicted, gave a method to address the problem.

MEANING OF ARTIFICIAL INTELLIGENCE

Artificial intelligence (AI) is a discipline of computer science that is rapidly evolving. In the mid-1950s, John McCarthy, dubbed the Father of AI," defined it as "*the science and engineering of making intelligent robots.*" Artificial intelligence (AI) is described as a machine's ability to perceive and respond to its surroundings without requiring direct human interaction, as well as to do activities that would ordinarily need human intelligence and decision-making processes.[1]

[1] Cath C.(2018) Governing artificial intelligence: ethical, legal and technical opportunities and challenges. *Phil.Trans. Royal. Society*, issue 2133, pp. 1–8.

Artificial intelligence (AI) is a sort of computer programme that can do tasks that would otherwise necessitate the use of human intelligence. Machine learning is used in several of these artificial intelligence systems, while deep learning is used in others, and rules are used in yet others. This is a result of learning, which entails gathering the rules and information needed to use the data. It has become increasingly popular and necessary as a result of data-based service sectors. Artificial Intelligence (AI) is a term that refers to machine intelligence rather than human intelligence. The study of "intelligent agents," or systems that understand their surroundings and take actions that maximize their chances of achieving their goals, as defined by leading AI textbooks.

Since its inception as academic research in 1956, artificial intelligence has gone through many phases of optimism, disappointment, and funding loss, followed by new techniques, success, and renewed funding. Artificial intelligence. A variety of approaches have been tried and rejected since the beginning of AI research, including brain mimicking, human problem-solving modelling, formal logic and enormous knowledge libraries, and animal behavior imitation. Mathematical statistical machine learning was the dominant approach to solving difficult problems in industry and academia in the first decades of the twenty-first century.

Although there have been abundant definitions of artificial intelligence (AI) throughout the earlier few decades, John McCarthy acclaims the following concept in this 2004 paper. "*It is the art and science of creating intelligent machines, particularly intelligent computer programmes. It's akin to the task of utilizing computers to study human intellect, but AI doesn't have to be limited to physiologically observable methods.*"

The computer must learn how to respond to specific behaviors, so it builds a propensity model using algorithms and historical data. We unintentionally profit from AI every day. As an example-

- Search engines are always making assumptions about what we're looking for as soon as we begin typing in a single letter.
- If you view videos in a certain genre, YouTube begins to recommend videos of the same type.

EFFECT OF ARTIFICIAL INTELLIGENCE

Artificial intelligence is a technology that is having a good impact on our lives and is also playing a role in our daily lives, such as reminding us of meetings and suggesting articles and news that we might be interested in. Its impact is projected to spread across entire database businesses as soon as possible. Artificial intelligence (AI) has the potential to have a significant impact on how people interact with one another, with the digital world, at work, and in other social and economic settings. If we are to ensure that artificial intelligence has a good influence, it is imperative that all stakeholders participate in the debates.

ROLE OF ARTIFICIAL INTELLIGENCE IN THE CRIMINAL JUSTICE SYSTEM

Artificial intelligence has demonstrated its ability to solve many of the world's most important problems while also enhancing our daily lives during the last few decades. AI's potential to benefit mankind is limitless, from self-driving cars to facial recognition software and tumour detection algorithms. According to market research firm IDC, the global market for artificial intelligence is expected to reach a value of about half a trillion dollars by 2024, implying that this incredibly powerful technology will continue to gain traction across a variety of industries. The criminal justice system is one of the most exciting applications of AI. Artificial intelligence (AI) can help judges analyze a defendant's risk and make sentence decisions. Artificial intelligence (AI) applications are, understandably, divisive. However, major social and ethical considerations, such as transparency and consistency, must be considered. These concerns must be addressed if AI is to be utilized effectively to assist judges in sentencing decisions and provide accurate evaluations of criminals' danger and requirements. Continue reading to discover more about how artificial intelligence (AI) is employed in the legal system, where and how AI technologies may be useful, and how issues like transparency, discrimination, and personal data privacy can be addressed.

In India, artificial intelligence in law enforcement is still in its early phases. Regardless, given our country's understaffed and underpaid police force, efforts are always being made to integrate AI into policing. A video investigation stage, JARVIS or Joint AI Research for Video Instances and Streams, was sent to Uttar Pradesh by Staqu, a Gurugram-based corporation that was created in 2019 [2]. As a result, JARVIS has been examining CCTV footage from all throughout the state since that time in order to compile a series of reports covering anything from violent crime scenes to pickpocketing swarms. When it comes to checking inmates for criminal activity in jails across Uttar Pradesh, JARVIS has proven to be a very beneficial tool. In addition to JARVIS, Punjab and Uttar Pradesh police forces are using PAIS and TRINETRA, respectively. As a database of over 35,000 criminals, PAIS (Police AI System) helps police identify and prevent wrongdoing. The FICCI Smart Policing Award was given to the Punjab Police Department in 2018 for its implementation of this strategy in a number of low- and high-profile cases. More than 5 lakh people's data have been acquired from all throughout the state 2018.[3]. More than 5 lakh people's data have been acquired from all throughout the state. However, Delhi police are utilizing Innefu Lab's facial recognition software to enhance its law enforcement tools in the interim period. In addition, the Delhi Police is using the Crime Mapping, Analytics, and Predictive System (CMAPS) to identify crime hotspots in the city. Foreseeing hot spots for criminal activity in the city is made easier with CMAPS, which analyses past data and calls to the police hotline. The CCTV Mannequin framework, which was introduced in Bangalore, is another recent advancement in the industry. These life-size figures, dressed as police officers, will be on the lookout for minor criminal infractions such as speeding and violating traffic laws. According to the Internet Freedom Foundation, experts in 19 states and association domains are currently using 48+ facial recognition frameworks, with Delhi having the most of these frameworks.[4]

IMPACT OF ARTIFICIAL INTELLIGENCE ON JUDICIARY

[2] Swati Sudhakaran,"How AI can be used in policing to reform criminal justice system", *The Print,* 21, March, 2020

[3] Hauck R. et al (2002) Using Coplink to analyze criminal-justice data. *Computer*, no 3, pp. 30–37.

[4] Retrieved from https://www.indiatoday.in/india/story/supreme-court-india-sc-ai-artificial-intellegence-portal-supace-launch-1788098-2021-04-07, Last visited on 25.01.2022

According to Oxford Insights and the International Development Research Centre, India ranks 17th on the government's artificial intelligence preparedness index. Five countries in descending order are Singapore, the United Kingdom, Germany, United States of America, and Helsinki. In 2020, a coronavirus outbreak forced the global community to come to a screeching halt. The Supreme Court, on the other hand, could not afford to stop all of its work given the current state of the court's cases. Thus, the Supreme Court created the SCI-Interact website to eliminate paper from all 17 of its benches. Additionally, a web-based infrastructure comparable to LIMBS would allow for more transparent digital case monitoring. The Supreme Court Portal for Courts Efficiency, India's first AI platform, was unveiled on April 6th, 2021 by the Supreme Court of India (SUPACE). Judges' workloads are expected to be reduced. Tests conducted by the Supreme Court have been extensive in order to make things simple and understandable.[5]

Role of SUPACE in the courts

"*They won't let AI spill over into decision making*," India's Chief Justice S.A. Bobde remarked. It's vital to note that in each scenario that makes A multitude of documents are generated on the path to a high court or the Supreme Court including the charge sheet, orders, subordinate court judgments, and so on. Going through all of these documents again to uncover important information is a time-consuming task. The justice system is slowed and inefficient as a result of this entire procedure. SUPACE will be useful in this situation. AI will go through the data the most essential faces and concerns presented by the parties and provide relevant data to the judges in order for them to make a decision. It will aid in legal research and the tracking of a lawsuit's progress. It will not, however, participate in decision-making. [6]

Presumably, A is a Supreme Court justice with four sessions scheduled each day. Each hearing is at a different point in the process, with a distinct set of facts. AI will aid in the process by providing all relevant facts to the court, ensuring that the judge does not have to bury himself beneath a mountain of files.

It will also facilitate legal research and provide other benefits to ensure that cases are resolved in a timely manner.[7]

The SUPACE portal for criminal cases has been in the high court of Bombay and Delhi, it was first implemented as a pilot programme. A committee is also looking into how artificial intelligence may be utilized to deal with motor accident claims tribunals. [8]

CONCLUSION

The criminal justice system in India is built on the premise that no one should be convicted of a crime for

[5] Retrieved from https://www.revlocal.com/resources/library/blog/what-is-ai-and-how-does-it-work

[6] Marda V. (2018) Artificial intelligence policy in India: a framework for engaging the limits of data-driven decision-making. *Philosophical Transactions of the Royal Society: Mathematical, Physical and Engineering Sciences*, vol. 376, pp. 1–19.

[7] Raschka S. et al (2020) Machine Learning in Python: Main developments and technology trends in data science, machine learning, and artificial intelligence. *Information*, no 4, p. 193.

[8] Retrieved from https://www.oxfordinsights.com/ai-readiness2019, Last visited on 25.01.2022

which they are not guilty, even if 100 guilty individuals are acquitted. Programming AI should take into account all of these concerns. In 2020, we demonstrated how the world could drastically change in just a few short months. AI's positive or negative impact on India will be decided by the country's citizens. It's impossible to ignore the fact that millions of people are anxiously awaiting a favourable court decision. It is impossible to refute that people are in debt due to lengthy court proceedings and exorbitant legal bills. As a result, judges and those involved in the legal system must see AI as a key to the future and work with it.

AI has risen to astounding heights thanks to a four-decade-old fixation on its advancements. In other words, key authoritative breakthroughs have failed to closely monitor the trend. Artificial Intelligence (AI) advances could easily be used in ways that conflict with popular culture's notions because of legal loopholes. It's possible that misuse of artificial intelligence could violate basic civil rights including the right to protection, the right to be free of separation, and the right to freely express oneself verbally and articulately. In India, the field of artificial intelligence, in particular for law enforcement, is still developing. Various focus-supported initiatives have been used by the Indian government to quickly embrace and advance this technology. There are currently no standards or norms in place to govern this new technology. AI findings have aroused a major international reaction because of their foggy and incomprehensible character. Several of these systems have been examined for unfair practices in the United States. People's Human Rights are jeopardized if criminal law enforcement lacks transparency.

14

LEGAL CHALLENGES ARISING WITH ARTIFICIAL INTELLIGENCE

KEYWORDS

ARTIFICIAL INTELLIGENCE, CYBER SECURITY, CYBER LAWS, TELSA CAR, AMAZON ALEXA, FACEBOOK

CHAPTER FOURTEEN

LEGAL CHALLENGES ARISING WITH ARTIFICIAL INTELLIGENCE

AUTHOR

MANASA M, LLM (CORPORATE AND COMMERCIAL LAWS)

ABSTRACT

It is indisputable that the world stands on the ground of faith in the justice system. It won't be an understatement to say that the steel curtains of development frequently blind us from the ethical world. The ability of a robot or a computer to discrete, procreate, and absorb from the actions of a human without any assistance has made lives less effortful. This dependency on Artificial Intelligence might have made the going smooth but the same has taken a toll on the rights and privacy of man. The understanding of the same and the need for its regulations shall be the sole **purpose** of this research.

A mixed form of **research** shall be used in the paper to gain the required results. The facts and sensational cases shall form the foundation whereas, the legal reforms and the need for regulating the statutes shall build the paper. The pre-existing laws and regulatory bodies around the globe and their legitimate implementation as per the norms of this country to achieve betterment in handling the outburst of technological misuse or overuse shall be the target of the research.

This research paper shall **consist** of the era's unpredicted legal challenges that are emerging along with the growth in technology and the need for an ordinance to govern the same.

The paper shall include cases and instances like the Google assistant's privacy deprivation, Alexa home assistant's Tracking issue, data storage issue, Tesla self-drive car hacking issues, etc.

Concluding, it shall consist of the views of the author regarding regulatory actions to fence the outburst of technological innovations and the crimes and deprivation of rights arising henceforth.

INTRODUCTION

It is indisputable that the world stands on the ground of faith in the justice system. The motive of the justice system in this world is to predict, protect, and take necessary precautions of any action that has been or shall be created by man, which will affect him or anything around him, directly or indirectly. This rapidly growing universe has made the up-gradation of the justice system a very challenging task. A new form of crime or an offense has been taking birth every time we keep a new step towards development.

It is very unfortunate to say that the old school justice system fails to run at the same speed as development today. Man has been blindfolded by the hands of Technology and has been unaware of the depth of the pond he has stepped into.

The fascinating Tech-world has been very successful in drawing the attention of commoners and leading them to be bound by the irresistible arms of assistance. It shall be very unfair to say that the development of Technology has not made life easy, but at the same time, it has given a hard time to the justice system in the world. Hence it won't be an understatement to say that the steel curtains of development frequently blind us from the ethical world. The ability of a robot or a computer to discrete, procreate, and absorb from the actions of a human without any assistance has made lives less effortful.

Artificial intelligence in layman's language can be called the theoretical and practical development of computer systems, by providing it an ability to perform human tasks at ease. Such functions shall include decision-making skills, speech recognition, facial recognition, and thinking abilities as an individual. This dependency on Artificial Intelligence might have made the going smooth but the same has taken a toll on the rights and privacy of man.

The advancement in technology has made it necessary for the judicial system to be updated with the new world that has evolved to be better every day. The laws and statutes governing the same must go hand in hand with the progress made on a day-to-day basis.

The challenges that are faced by the legislative system to keep up with this rapidly growing technology shall be discussed along with case laws and instances in this paper.

DEPENDENCE OF HUMANS ON TECHNOLOGY

Nowadays it is almost impossible to lead a life that has not been acquired by technology. Fortunately, or unfortunately, humans today are dependent upon technology from bed to bed. There has been a saying that too much is too bad which will be applicable in this scenario as well. The sole purpose of the adaptation of Technology has been to ease the day-to-day chores and make them less time-consuming. But the problem arises with the Collateral Damage that has been cost as an action of the development of such technology.

Speaking about the Collateral Damage that shall be caused as a shadow to the adaptation, development, and dependency of Technology, the graph of the same has been spiking up at a very usual rate leading to unpredicted side effects. These side effects have been a challenge not only to the adapter of the technology but also to the legal system and the government which thrives to run a crime free and a disturbance free society.

There have been many incidents which have made us realise the Collateral Damage that can be caused as an effect of outburst in technological development.

The following shall be few such incidents which have brought a challenge is the legal system around the globe through its innovative problems.

INCIDENT 1.

Facebook data theft case:

On March 16 2018 The New York Times And the Guardian reported that a data-mining firm named "Cambridge Analytica", which had worked for Donald Trump's presidential campaign had improperly obtained access to more than 50 Million user profiles.

Experts believe that the firm could have used that data to gain an unfair advantage in targeting voters. It came to the view that there was no person behind such a data theft but the company using artificial intelligence, where the technology on its own could record the likes and dislikes of the profile holders in Facebook without any knowledge of the user. It was known that "Cambridge Analytica" had the details of over 50 Million Facebook users for 2 years and was constantly updated. Such an act is called psychographic profiling, which helps in persuading voters.

Immediately an investigation was called on Facebook by the FTC. This has been not only a violation of a person's privacy but also an illegal way to impose political ideologies during election campaigns in a democratic country.

The CEO of Facebook Mark Zuckerberg was called by the Senate Commerce and Judiciary committee on April 10th, 2018 to discuss "data privacy and Russian disinformation" and was held guilty. Including multiple Court cases in the US, the court fined Facebook 3-5 Billion US dollars and stated that in data privacy cases the action cannot be undone and hence there shall be no imprisonment but just a Monetary fine.

INCIDENT 2.

Tesla car hacking case:

One of the most shocking and dangerous misuses of artificial intelligence has been seen in the incident of Tesla car hacking. We all know that the company Tesla has portrayed itself as the future of the transportation and automobile industry of the world. Self-driven cars and electrically powered vehicles have brought a humongous change in the idea of automobiles in the world.

The Tesla Company has been striving hard to improve their internal security and strengthen the walls of their AI because these electric cars have been hacked many times before. But a recent incident where a German teenager hacked about 25 teslas without any direct contact to the cars and took complete control over the cars through a third-party app, questions not only the privacy but also the safety of such artificial intelligence. When it comes to the automobile industry, the sole purpose of any vehicle shall be serving road safety. but in this incident, it was prominent that the same shall not be served if the work of a man shall be handled by artificial intelligence.

Even though the company took complete responsibility for the action and made necessary arrangements to not repeat the same, it is still skeptical to blindly hand over the lives of the driver as well as innocent people into the hands of artificial intelligence.

INCIDENT 3.

Alexa overhearing case and improper response case:

The home assistant Alexa has been a part of most of the families around the world in easy completion of their day-to-day work. but the question arises as to how safe are our conversations and data that we are producing into Alexa with or without our knowledge. There have been many instances where Alexa has been accused of eavesdropping and collecting personal data of the people around her without any permission or knowledge of the humans. There have been more than 8000 incidents recorded with either appropriate replies by the AI or unexpected replies in between conversations that do not involve Alexa.

This AI is also accused to have been recording the conversation without permission. Incidents where the human has stopped Alexa by telling "Alexa, stop recording" without a prior command of "Alexa, start recording".

In one of the cases, a couple in Portland, Oregon was sent random recordings of their private conversation by Alexa, which panicked the couple and made them realize that Alexa has a brain of our own and it is not just an assistant who works as per the command of the owner but shall work as per its convenience. This is an alarming misuse of human dependence on artificial intelligence.

INCIDENT 4.

Citizenship issue with AI:

Fortunately, or unfortunately there have been mind-blowing inventions in the field of Artificial Intelligence and Technology, where a robot shall have 90% of the capacities humans possess. The capability of an AI to think and respond accordingly to any conversation proves that the same shall have the capacity to be called an individual.

One such AI has been named Sophia. In 2017 the robotic company named "Hanson robotics" manufactured an Ultra humanized and developed version of a robot that could think, respond, recollect, memories and react to any human interactions just like an average human being. The robot also had physical appearance features of a female body along with bodily mannerisms of a human being like blinking of Eyes, handshakes, smiling, and gestures. With such advancement, the manufacturing company claimed it to be an individual and applied for its citizenship.

Speaking legally in countries like India citizenship shall be obtained only by human beings either by birth or any other way as mentioned in the statutes. But, Sophia was granted Saudi Arabian citizenship in the year 2017. This was the first time a robot broke the walls to enter the humanoid with its intellectual capability.

It is very questionable if the near Intelligence and appearance of an AI shall lead them to be considered as one among the human species. We have never seen citizenship granted to any animal with as much intellect as a human, and hence it is tricky to call a man's creation with artificial or imposed intelligence a citizen of a nation.

REGULATORY LAWS IN INDIA AND THEIR SUSTAINABILITY

Taking into consideration the above incidents and their gravity towards the cause of various crimes towards innocent people, let us look at the practicality of laws to govern the same.

Even though the above-mentioned crimes have not been caused in India, the same shall not take a long time to set its foot into the soil of this country. The outburst in the technological field in India has beeped an alarm to the legal system. Currently, in India, there are only fuse laws that govern artificial intelligence or any other technological development and the Collateral Damage that has been caused by the over-dependency of humans on such Technology. Among such statutes, the Information Technology Act of 2000, takes the majority space. But the question is to what extent does the Act support the misuse of the development in technology.

Let us look into a few of the drawbacks when it comes to the sustainability of such laws in India.

1. The growth rate of Technology and the rate at which the statutes have been updated shall not go hand in hand. This can lead to outdated laws and hence unanswerable questions.
2. The lack of knowledge among the executives, to file Complaints against such offenses.
3. The lack of understanding of technology by the Judiciary shall lead to partial solutions in any judgments.
4. The legislative fail in drafting laws that shall cover anticipated misuse of Technology.

These are a few of the reasons India is a step back when it comes to taking regulatory steps in the field of Artificial Intelligence and its development in this country.

CONCLUSION

There is a saying that too much is too bad, which will be very apt for this situation. The exploding development and Technology have made human life moves smoother but at the same time, the risk to lose privacy and being a victim of unknown and unpredicted crimes spike up very high.

Today it is almost impossible for us to not depend on artificial intelligence and hence the only way out of such issues is to bring appropriate regulations in the statutes of the nation and avoid further crimes.

The deprivation of the right to privacy shall be the deprivation of a fundamental right that makes it the responsibility of the state to handle the incident. The other crimes that collaterally occur with extreme dependency on Technology need to be governed under the criminal procedure in a fair manner. All these can be done only if all the three pillars of the state have sufficient knowledge about such Technology and can predict the outcomes of the same.

REFERENCES

1. Gautam, R., Kulshrestha, P., & Goswami, M. A. K. (2021). Mediation And Family Dispute Resolution Mechanism: A Case Study On Clinical Legal Education. Elementary Education Online, 20(3), 2490-2490.

2. Gautam, R., "Proliferation of Cyber Crime and Indian legal system with special reference to Gwalior Division" Available at: https://shodhganga.inflibnet.ac.in/handle/10603/250817 Retrieved on: 22/07/2021

3. Pandey, N., Gautam, R., "property right of women in patriarchal indian society: a comprehensive study on legal narrative" Available at: https://www.researchgate.net/publication/361733554_PROPERTY_RIGHT_OF_WOMEN_IN_PATRIARCHAL_INDIAN_SOCIETY_A_COMPREHENSIVE_STUDY_ON_LEGAL_NARRATIVE_PROPERTY_RIGHT_OF_WOMEN_IN_PATRIARCHAL_INDIAN_SOCIETY_A_COMPREHENSIVE_STUDY_ON_LEGAL_NARRATIVE

4. Gautam, R., Medical health condition of prisoners and discrepancy in facilities among the states of Uttar Pradesh, Haryana and Delhi, International Journal of Health Sciences Follow journal, DOI: 10.53730/ijhs.v6nS6.12256

5. Gautam, R., Kanpur Philosophers ISSN 2348-8301 Vol IX, Issue V (IV), 2022151EFFICACY OF PROCEEDINGS OF CONCILIATION AND SETTLEMENT OF ANINDUSTRIAL DISPUTE UNDER INDUSTRIAL DISPUTES ACT, 1947, A CRITICAL Analysis. Available from: https://www.researchgate.net/publication/361733673_Kanpur_Philosophers_ISSN [accessed Sep 11 2022].

6. Gautam, Ritu, Cybercrimes and International legal regime, Available at: https://shodhganga.inflibnet.ac.in/bitstream/10603/250817/10/10_chapter-iv%20%20cybercrime%20issues%20and%20international%20legal%20regime.pdf

7. Gautam, Ritu, Cyber crime in India, Availablr at: http://hdl.handle.net/10603/250817

15

CYBER CRIME, SECURITY AND REGULATION IN INDIA

KEYWORDS

INSURANCE, IT ACT, ETHICAL HACKING, FIXATION, PORNOGRAPHY SITE ATTACK

CHAPTER FIFTEEN

CYBER CRIME, SECURITY AND REGULATION IN INDIA

AUTHORS

VINITA SINGH, PH. D SCHOLAR, SCHOOL OF LAW, SHARDA UNIVERSITY, INDIA

DR RITU GAUTAM, ASSISTANT PROFESSOR, SCHOOL OF LAW, SHARDA UNIVERSITY, INDIA

ABSTRACT

In India every single moment one individual become internet users. Its union with carefully upheld stages and devices, shielding the guardians as well as understudies from the cybercrimes is turning into a challenging task. Notwithstanding, the squeezing the truth is that the internet user are not getting refreshed on the helpless Digital dangers and security issues, at the speed they are getting refreshed with the utilization of web empowered instruments Also applications. In this manner the momentum research paper centres in Discovering the responses to disturbing inquiries – "Is the Netizen truly mindful that he/she is defenceless against different Digital wrongdoings?"; "Assuming netizen knows, how much?". "If Not mindful of cybercrimes, what measures can be taken on To make the citizens more mindful and refreshed. The paper Recommended a theoretical model disclosing how to maintain What's more execute the mindfulness programs among internet user in regards to cybercrimes.

INTRODUCTION

The world isn't controlled by weapons any more or energy or Cash, it is controlled by ones and zeroes-small amounts of information. It is all Electrons. There is a conflict out a universal conflict. There's no need to focus on who has the most BULLETS. It is concerning who controls the data. What we see and hear, how we work, what we see, it is about Data or information.

No words can all the more likely depict the current situation of technology than above expressed by universe the lowlife in the film "sneaker".

Cyber crime is a criminal behaviour that is carried out by utilizing a PC or the Internet. Cyber crime incorporates charge card and ledger misrepresentation, programming robbery, copyright encroachment, following and provocation. Malignant programming (malware) is regularly concealed in innocuous looking email connections. Phishing tricks are intended to fool Internet clients into sharing passwords and other private information. Cyber wrongdoing can be perpetrated against individuals, property and associations. Persistent observing of PC networks is important to safeguard delicate data. Digital wrongdoings or cyber crime against people incorporate spam and satire email, criticism, badgering and following. A farce email is one that has all the earmarks of being from an unexpected source in comparison to the genuine originator. Spam email is numerous duplicates of a similar email, for example, junk messages or deals requesting. Digital maligning is submitted when somebody distributes claims on a site or through email. Digital following happens when somebody utilizes visit rooms, email and long-range informal communication destinations to screen someone else's Internet action and participate in unwanted contact.

Digital wrongdoing or cybercrime against property incorporates charge card misrepresentation, programming robbery and data transfer capacity burglary. Digital hoodlums get credit card information by connecting malware to email. Phishing is utilized to trick a person into giving private data. Phishing messages and websites frequently seem real. They might show the authority logo of a monetary organization. Robbery of transmission capacity is unapproved admittance to an Internet association. Programming theft is replicating and dispersing protected programming. Sharing "breaks" and key generators to bypass software assurance is viewed as programming theft.

Progressed determined dangers are proceeding with covertness assaults against an association. Government offices are as often as possible the objective of this

Sort of digital wrongdoing. Digital hoodlums ordinarily approach a protected information organization or office site for quite a long time before they are found.

During this time, the digital crook approaches secret data. Digital hoodlums utilize uniquely composed PC code to recover information without location by firewalls. Progressed steady

Dangers incorporate different states and political gatherings taking part in secret activities.

"Hacktivism is a new advancement in Internet security.

Hacktivism is a type of digital activism to dissent or to acquire data to be utilized by a gathering went against to the objective site. Hacktivists get entrance to private or government data sets and sites to acquire classified data or disturb the site. Hacktivists might close down a site in dissent of government strategy or business movement. Sites might be seized to propel a political or social plan. Hacktivists are for the most part efficient and have the high-level coding abilities important to Get delicate data".

The results of PC wrongdoing are colossal as far as both the financial expenses as well as human security. Since the web gives many benefits to the crooks to submit following kinds of wrongdoing: -

- Wrongdoing or cyber influencing people.
- Wrongdoing or cyber influencing economy.
- Wrongdoing or cyber influencing public safety.
- Licensed innovation freedoms.

There are the two sorts of criminal liabilities beyond a shadow of a doubt exercises. Digital violations are led on the remote organization through PC programming. An assortment of administrations is impacted by the digital wrongdoings. Not just business people as well as shoppers are likewise extremely impacted due to the digital violations.

The term web extortion is extremely exhaustive yet has not been explicitly characterized under the demonstration Information Technology 2000. The fakes through web will take an assortment of structures in their grouping can't be effortlessly kept up with however the principal reason for this exploration work is to discover the security status also what are the issues which is should have been tended to earnestly with regards to the security of exchange, protection, banking extortion, property furthermore different issues.

"Each spending day saw new advancements in the PC Innovation. The PCs with fresher capacities have been created. These PCs have astonishing velocity and putting away limit. They Fill now diverse roles. Accordingly, rather than being litigant on bureaux, many organizations bought their own PCs, with the result numerous bureaux began to enhance, consistently moved into the programming field or searched for specialty markets.

HISTORY OF CYBER CRIMES

"The originally recorded digital wrongdoing occurred in the year 1820! That isn't shocking considering the way that the math device, which is thought to be the earliest type of a PC, has been around beginning around 3500 B.C.

In India, Japan and China. The period of modem PCs, be that as it may, started with the scientific motor of Charles Babbage".

"In 1820, Joseph-Marie Jacquard, a material maker in France, delivered the loom. This gadget permitted the reiteration of a series of steps in the winding around of special textures. This brought about a dread among Jacquard's representatives that their customary work and Vocation were being compromised. They submitted demonstrations of treachery to deter Jacquard from additional utilization of the new innovation. This is the First recorded digital crime".

"Digital wrongdoing is an evil having its starting point in the developing reliance on PCs in modem life. In a day and age when everything from microwaves and coolers to thermal energy stations is being mn on PCs, digital wrongdoing has expected rather vile ramifications. Major digital wrongdoings in the new past incorporate the Citibank rip off. US $ 10 million were deceitfully moved out of the bank and into a financial balance in Switzerland. A Russian programmer bunch drove by Vladimir Kevin, a famous programmer, executed the assault. The gathering compromised the bank's security frameworks. Vladimir was purportedly utilizing his office PC at AO Saturn, a PC firm in St. Petersburg, Russia, to break into Citibank PCs. He was at long last captured on Heathrow air terminal on his way to Switzerland.

IMPORTANCE OF CYBER CRIMES

In this day and age, there is a tremendous expansion in the utilization of Web or internet in each field of the society and because of this increment in use of Web, various new wrongdoings have involved. Such violations where utilization of PCs combined with the utilization of Internet is involved are extensively named as Cyber Crimes.

In any case, under Indian regulation "Cybercrime" as such has not been characterized under any regulation. One regulation that arrangements with the offenses connected with such violations in India is Information Technology Act, 2000,

Which was additionally changed in the structure of IT Amendment Act,2008. In any case, these two significant regulations additionally do exclude any definition for "cybercrime". Whenever investigated common sense, it isn't at all simple to characterize this term.

To characterize such an offense, when the nature of such offense is seen, it is a mix of wrongdoing and PC. Thus, one might say that, when in commission of any offense PC is utilized, that can be named as "digital crime".

In our Indian Information Technology Act 2000, PC Has characterized in expansive term as –

PC implies any electronic attractive, optical or other high Speed information handling gadget or framework which performs consistent, number-crunching, and memory capacities by controls of electronic, attractive or optical motivations, and incorporates all input, yield, handling, capacity, PC programming, or correspondence offices which are associated or connected with the PC in a PC framework or PC network. The significance of digital wrongdoing isn't profoundly not quite the same as the significance of regular wrongdoing. Both incorporate lead whether act or oversight which cause break of rules of regulation and offset the authorization of the state. Prior to assessing the importance of digital wrongdoing, it is must to examine about regular crime.

“Wrongdoing is a social and financial peculiarity and is pretty much as old as the Human culture, “digital wrongdoing might be supposed to be those types of which class is the regular wrongdoing and where either the PC is an article or subject of the direct comprising wrongdoing”. “Any lawbreaker action that utilizes a PC either as an instrumentality, target or a implies for sustaining further violations goes inside the ambit off Digital crime”

It implies we can say that violations which are directed through the PC is called digital wrongdoings, it’s unlawful which are carried out in a Network climate or on web. In this specific circumstance if any individual carries out a digital wrongdoing is known as digital crook.

The digital law breakers might be youngsters and juvenile matured beneath 6-18 years it could be conceivable that they are proficient programmers or coordinated, con artists or mystic people are additionally might be digital hoodlums.

Presently, it has turned into the extraordinary concern of the world over due to our reliance on PCs have been expanded. Nearly it has become consistently story that some sites which are vital, have been captured or infection harmed the framework, it is likewise used to take a individual’s character. It is a sort of wrongdoing which occurs in the internet. A virtual World made by humanity utilizing PCs and systems administration.

“Digital wrongdoings are any violations that include a PC and a Network. Now and again, the PC might have been utilized to perpetrate the wrongdoing, and in different cases, the PC might have been the target of the crime”.

“Digital wrongdoing includes any crook act managing PC and organizations called hacking. Moreover, digital wrongdoing too Incorporates customarily violations directed through the web. For Model; disdain wrongdoings, selling and web extortion, fraud, also charge card account robberies are viewed as digital wrongdoings when the criminal operations are carried out using a PC and the internet”. In the field of the internet digital wrongdoing is the new arising Species, new types of hoodlums, they are engaged with upsetting the Business and administrative interests.

A Cyber wrongdoing alludes to every one of the exercises finished with criminal plan in the internet. As a result of unknown nature of the web, it is conceivable to draw in into an assortment of crimes without risk of punishment. Individuals with insight have been terribly abusing this part of the web to sustain crimes in the internet “Digital wrongdoing is referred to all around the world as a wrongdoing Submitted through web. It is, these days, turning into a big deal of concern from one side of the planet to the other. The idea of digital wrongdoing is like a new Type of a show wrongdoing, if we talk about the utilization of web then we Observe that it isn’t quite so wide as other fostered nations’ wrongdoing, in any case, connected with web is in arising stage thus this country. The review is exploratory in nature. Systemic triangulation (eye to eye meeting and contextual investigation) has been applied to gather relevant information from purposively chosen respondents. It is uncovered from the review that, however digital wrongdoing isn’t in not kidding condition in research region, the respondents are deceived at some point by programmer, sexual entertainment locales and PC infection through web. It is consistently developing consideration of the larger part individuals of the study area".

There is nobody is really proprietor of the web and no single individual or association controls the web in its element. In this way there is no unified administration in either innovative execution or Arrangements for about the use and access.

"The term web and World Wide Web {WWW} are frequently Utilized conversely in ordinary discourse; it is normal to talk about "going on the web" while conjuring a program to see Web pages. Be that as it may, the web isn't inseparable from World Wide Web".

NATURE OF CYBER CRIMES

This part gives some foundation data on PC wrongdoing, for example, which kinds of PC wrongdoing appear to happen most frequently, and how it has been forestalled up until this point. In truth, PC wrongdoing is changed, maybe much more than our unique definition proposes.

Correspondingly, an endeavour to control it has differed too. It appears to be genuinely clear, in light of episodic proof that extortion, Youngster sexual entertainment, unapproved access, and related violations make up most of PC wrongdoing". Digital wrongdoing is an always present danger with a consistently evolving face.

The computerized age has led to another variety of abundance tracker. While their usual methodology and hardware might contrast significantly with that of their awful ancestors, their intention is something very similar – prompt acquire to another's detriment.

Digital wrongdoing is changing, not just in the profile of the hoodlums Very not the same as what we have since quite a while ago comprehended to be the situation, their inspiration and methods have created and are more modern What's more vile. People and organizations must be proactive in their way to deal with safeguard as indicated by the most recent release of the Symantec Internet Security Danger Report, assaults and noxious code rule digital wrongdoing and the objective has moved from being the organization edge and is presently Internet browsers and Web applications. Assailants are not generally confined pockets of for the most part confused people whose central point is to test abilities against security frameworks or carefully trespass and mutilate sites.

Today, digital lawbreakers are coordinated and, generally speaking piece of syndicates, laid out to do dangers to separate data for misrepresentation, coercion and other lawbreaker acts. The overall pattern focuses to an expansion in weaknesses and organizations are being compelled to address this issue across the framework.

Other calming realities archived in the report incorporate Symantec Having hindered 1,5 billion phishing endeavour's, addressing a 44% Increment over the principal half of 2005; and a normal of 7,9 million Phishing endeavour's each day – an increment of 39%. As far as danger movement for the period July to December 2005 is concerned, Symantec has taken note of the pursuing key directions, among others.

The incorporation of innovation and frameworks should take into Thought basic business prerequisites and join the jobs of individuals, cycles and strategies. Digital wrongdoing is whether legend or reality? Nothing is wrongdoing except if recommended by regulation. Be that as it may, the greater part of the classifications of digital wrongdoing is still past the range of regulation. Indeed, even there is absence of consistent agreement. Above lines has endeavoured to conceptualize the 'digital wrongdoing'. The investigation is from legitimate place of view and different viewpoints are addressed. A careless glace has been given to whether digital wrongdoing can be obliged inside the current lawful system or does it require a total new methodology? This term has investigated the functional methodology to battle digital wrongdoing and its plausible hardships in the conventional framework which depends on various standards, which in the internet barely regard and hard to administer. The goal of these investigations is to check the similarity of general set of laws to roadster up with such techno-refined culpability.

CYBERCRIME ATTACK TYPES

Cybercrime can assault in different ways. Here, is some most normal cybercrime assault mode:

Hacking:

It is a demonstration of acquiring unapproved admittance to a PC framework or organization.

Refusal Of Service Attack:

In this cyberattack, the digital lawbreaker utilizes the transfer speed of the casualty's organization or fills their email box with malicious mail. Here, the aim is to disturb their standard administrations.

Programming Piracy:

Robbery of programming by wrongfully duplicating real projects or falsifying. It likewise incorporates the dispersion of items planned to pass for the first.

Phishing:

Phishing is a strategy of removing classified data from the bank/monetary institutional record holders by illicit ways.

Satirizing:

It is a demonstration of getting one PC framework or an organization to profess to have the personality of another PC. It is generally used to gain admittance to restrictive honours appreciated by that organization or PC.

DIGITAL CRIME TOOLS

There are many sorts of Digital criminological devices

- **Kali Linux:**

Kali Linux is an open-source programming that is kept up with and supported by Offensive Security. It is an extraordinarily planned program for computerized legal sciences and infiltration testing.

- **Ophcrack:**

This apparatus is principally utilized for breaking the hashes, which are produced by similar records of windows. It offers a solid GUI framework and permits you to runs on different stages.

- **Encase**:

This product permits an examiner to picture and look at information from hard circles and removable plates.

- **Safe Back:**

Safe Back is essentially utilizing for imaging the hard plates of Intel-based PC frameworks and re-establishing these pictures to a few other hard circles.

- **Information unloader:**

This is an order line PC legal apparatus. It is openly accessible for the UNIX Operating framework, which can make precise of plates reasonable for computerized legal examination.

- **Md5sum:**

A device to actually look at assists you with checking information is replicated to another capacity effectively or not.

NEED FOR CYBER LAW

In the present techno-wise climate, the world is turning out to be increasingly more carefully modern as are the wrongdoings. Web was at first evolved as an exploration and data sharing instrument and was in an unregulated way. As the time elapsed by it turned out to be more value-based with e-business, web-based business, e-administration and e-obtainment and so forth All legitimate issues connected with web wrongdoing are managed through digital regulations. As the quantity of web clients is on the ascent, the requirement for digital regulations and their application has likewise built-up incredible speed.

In the present exceptionally digitalized world, nearly everybody is impacted by digital regulation.

World and Cyber Laws:

- The Great firewall of China screens each second in the internet and safeguard to distribute any hostile substance.
- China has a hang on each content which is unsafe of perilous for the public authority of China.

- Brazil is viewed as world’s greatest air terminal for Hackers.
- Iran is additionally a perilous country for the Netizens. He additionally has a Crime Police unit for wrongdoing in Cyber Space.

SIGNIFICANCE OF CYBER LAWS:

1. We are living in profoundly digitalized world.
2. All organizations rely on their PC organizations and keep their significant information in electronic structure.
3. structures including annual government forms, organization regulation structures and so on are currently filled in electronic structure.
4. Purchasers are progressively utilizing Visas for shopping.
5. The vast majority are utilizing email, PDAs and SMS messages for correspondence.
6. Indeed even in “non-digital wrongdoing” cases, significant proof is found in PCs/mobile phones for example in instances of separation, murder, capturing, coordinated wrongdoing, psychological oppressor activities, fake cash and so on
7. Since it contacts every one of the parts of exchanges and exercises on and concerning the Internet, the World Wide Web and Cyberspace consequently Cyber regulation is critical.

CONCLUSION

To summarize, however a wrongdoing free society is awesome and exists just in deception, it should be consistent endeavour of rules to keep the guilt’s most minimal. Particularly in a general public that is reliant increasingly more on innovation, wrongdoing in view of electronic regulation breaking will undoubtedly increment and the legislators need to exceed everyone’s expectations contrasted with the frauds, to keep them under control.

Innovation is generally a two-sided deal and can be utilized for both the reasons – fortunate or unfortunate. Steganography, Trojan Horse, Scavenging (and even Dos or DDos) are generally advancements and fundamentally not violations, but rather falling into some unacceptable hands with an unlawful aim who are out to take advantage of them or abuse them, they come into the variety of digital wrongdoing and become culpable offenses.

Thus, it should be the industrious endeavours of rulers and legislators to guarantee that innovation fills in a sound way and is utilized for legitimate and moral business development and not for carrying out violations. It should be the obligation of the three partners viz. I) the rulers, controllers, administrators and specialists ii)

Internet or Network Service Suppliers or banks and different arbiters and iii) the clients to deal with data security assuming their separate part inside the allowed restrictions and guaranteeing submission with the tradition that must be adhered to.

REFERENCE

1. www.internetlivestats.com, 2016
2. www.statista.com, 2016
3. M. Dasgupta, Cyber Crime in India- A Comparative Study (Eastern Law House, Lucknow, 2009).
4. D.S.Yadav, Foundation of Information Technology, (New Age International Pub. Ltd. New Delhi, 3rd edn., 2007)
5. Gautam, Ritu, Cybercrimes and International legal regime, Available at: https://shodhganga.inflibnet.ac.in/bitstream/10603/250817/10/10_chapter-iv%20%20cybercrime%20issues%20and%20international%20legal%20regime.pdf
6. Gautam, R., Kulshrestha, P., & Goswami, M. A. K. (2021). Mediation And Family Dispute Resolution Mechanism: A Case Study On Clinical Legal Education. Elementary Education Online, 20(3), 2490-2490.
7. Gautam, R., "Proliferation of Cyber Crime and Indian legal system with special reference to Gwalior Division" Available at: https://shodhganga.inflibnet.ac.in/handle/10603/250817 Retrieved on: 22/07/2021
8. Pandey, N., Gautam, R., "property right of women in patriarchal indian society: a comprehensive study on legal narrative" Available at: https://www.researchgate.net/publication/361733554_PROPERTY_RIGHT_OF_WOMEN_IN_PATRIARCHAL_INDIAN_SOCIETY_A_COMPREHENSIVE_STUDY_ON_LEGAL_NARRATIVE_PROPERTY_RIGHT_OF_WOMEN_IN_PATRIARCHAL_INDIAN_SOCIETY_A_COMPREHENSIVE_STUDY_ON_LEGAL_NARRATIVE
9. Gautam, R., Medical health condition of prisoners and discrepancy in facilities among the states of Uttar Pradesh, Haryana and Delhi, International Journal of Health Sciences Follow journal, DOI: 10.53730/ijhs.v6nS6.12256
10. Gautam, R., Kanpur Philosophers ISSN 2348-8301 Vol IX, Issue V (IV), 2022151EFFICACY OF PROCEEDINGS OF CONCILIATION AND SETTLEMENT OF ANINDUSTRIAL DISPUTE UNDER INDUSTRIAL DISPUTES ACT, 1947, A CRITICAL Analysis. Available from: https://www.researchgate.net/publication/361733673_Kanpur_Philosophers_ISSN [accessed Sep 11 2022].
11. Gautam, Ritu, Cybercrimes and International legal regime, Available at: https://shodhganga.inflibnet.ac.in/bitstream/10603/250817/10/10_chapter-iv%20%20cybercrime%20issues%20and%20international%20legal%20regime.pdf
12. Gautam, Ritu, Cyber crime in India, Availablr at: http://hdl.handle.net/10603/250817
13. Preventive Laws with Special Reference to India, (Central Law Agency Publication, Allahabad, 2010).
14. Dr.Amit Verma, Cyber Crimes in India (Central Law Publication, Publication, Allahabad, 2010)

16

A CRITICAL ANALYSIS OF LEGAL CHALLENGES OF E- CONTRACTS IN INDIA

KEYWORDS

CYBER SECURITY, E-CONTRACTS, INFORMATION TECHNOLOGY, ELECTRONIC COMMUNICATIONS, ELECTRONIC MEDIA

CHAPTER SIXTEEN

A CRITICAL ANALYSIS OF LEGAL CHALLENGES OF E- CONTRACTS IN INDIA

AUTHORS

MANMEET KAUR ARORA, RESEARCH SCHOLAR, SCHOOL OF LAW, SHARDA UNIVERSITY, INDIA

KIRAN KUMAR NIRDHALA, STUDENT (LLB), NIMT INSTITUTE OF LAW AND METHOD, UTTAR PRADESH, INDIA

DR. NITUJA SINGH, ASSISTANT PROFESSOR, SCHOOL OF LAW, SHARDA UNIVERSITY, INDIA

ABSTRACT

The Indian Economy stands on agriculture, banking, finance, manufacturing sector, business sector, etc. The e-governance in these sectors has gained new heights even in the pandemic. The constant threats and issues related to cyber security have plagued the system at every level, especially fraudulent E-contracts. Even the Reserve Bank of India has acknowledged the uncertainties regarding Cyber Securities for example Vishing, via Phishing, Remote Access, etc. This research attempts to study to prohibit fraud applications and loss of money by individuals and organizations by elucidating a toll-free model which can detect fraud exposure while entering into E-contracts for example Fraudulent Recruitment E- contracts. The aim of the research is to provide a major contribution represented in a reliable detection model using firewalls, e-contracts, legal awareness, and others. The detection of Online Recruitment Fraud is characterized by QR codes, OTP, tele verifications, and other studies on this concept. The researcher proposed the detection model to achieve the basics of cyber security. Furthermore, this study focuses on context formation agreed by the parties i.e. a valid offer and due acceptance with the line to e-contracts, however, the contracts should not be denied on any ground as data messages are used for the purpose according to Provision Sec 10A of IT Act 2000. Through this paper researcher will bring provisions of formation of the contract, quality communication, the validity of e-contract in light of the legal framework of Information Technology Act 2000 along with electronic communications, electronic media.

INTRODUCTION

Today the world is acknowledging the revolutionary upgradation through internet for communication, not only internet the individual successfully carrying out data exchange with another electronic medium. The e-business is the result of achieving shared trade and business goals. With the significant degree of web usage at different platforms of the world, and the number of web end users are increasing significantly, the web-based business is blasting. With the extraordinary speed and velocity and the limited geographical boundaries, the major advantages of the web have contributed a great deal to the development of online business. For example, a purchaser in India can purchase merchandise from a vendor in the China or any other part of world where internet connectivity is available with help of couple of applications or clicks of the mouse for instance Ali- Baba, Amazon etc., and that too without having to leave one's position. Another major achievement of web-based business communication in form of contracting in the electronic world known as an electronic contract or e-contract or online contracts. "End User License Agreement" or EULA where one has to click on the "I Agree" button to install a software or the Terms and Conditions/User Agreement on a website are two most common type of E-Contract which is been actively used by vast majority.

E-contract are considered as one leg of electronic commercial activities. It is like a customary business wherein different varieties of Goods, products, and services are exchanged for a specific measure of thought. The significant component included is that the agreement happens through an advanced method of correspondence. It gives an open door to the merchants to arrive at the finish of the buyer straightforwardly without the contribution of the mediators

An E-contract can be formed on the web-based medium after initiation by at least 2 parties with intent of Conesus ad- idem, the transaction will take place electronically, for example, email, the association of a person with an electronic specialist, for example, a PC program, or the involvement of not less than two electronic that are customized to perceive the presence of an agreement. The Indian Contract Act, 1872 oversees the way where agreements are made and acted in India.

E-CONTRACT AN OVERVIEW OF PRESENT SCENARIO

Considering what is happening in society due to the ongoing pandemic situations, an e-contract is perhaps the furthermost straightforward choice to go into an agreement. With late progressions in PC innovation, media communications innovation, programming, and data innovation, individuals' way of life has been changed in incomprehensible ways. Correspondence is not generally restricted because of topographical and fleeting limitations. More data is communicated and gotten than any other time. This is the place where electronic trade gives adaptability to the business climate as far as area, time, space, distance, and cash.

All fundamental components of agreement regulation apply similarly to contracts laid out electronically or orally. Individuals regularly question how old and traditional agreement regulation ideas apply to new and imaginative kinds of innovation, which makes a situation. Nonetheless, the fundamentals and elements of e-contracts continue as before as those of written agreements which are prevailing in current scenario. The fundamental principles, procedures of Indian Contract act apply indistinguishably to the E-contracts, the basic spirit of entering into an agreement is followed as it is while entering into e-contracts. Web-based business alludes to the buying and selling of data, items, and administrations through PC organizations. It is a strategy for leading business on the web, commonly over the Internet. It is the instrument that prompts 'project incorporation.' Therefore, with the extension of internet business comes a critical expansion in the utilization of web-based contracts.

Web-based contract is another wing of e-business. It is practically identical to conventional form business in that items and administrations are traded for a specific measure of cash. The foremost distinction is that the agreement is executed utilizing a computerized strategy for correspondence like the web.

TYPES OF E CONTRACT

The web-based agreement development utilizes a correspondence innovation that includes various mediators like Internet Service Providers (ISPs). Envision an agreement that an Indian exporter and an American merchant wish to go into. One choice would be that one party first pulls up two duplicates of the agreement, signs them, and dispatches them to the next, who thus signs the two duplicates and messengers one duplicate back. The other choice is that the two gatherings meet somewhere and sign the agreement.

The following is critical examination of types of E-contracts:

Shrink-wrap agreements:

Ordinarily, **Shrink-wrap** agreements are a permitting arrangement for programming buys. In the case of Shrink-wrap contracts, the agreements for admittance to such programming merchandise ought to be upheld by the individual buying it, with the beginning of the product item›s bundling. Straightening out arrangements are only the arrangements that buyers acknowledge, for example, Windows pc-suite, at the time of introducing the program based product on a CD-ROM. Extra condition could just be seen at the start of introducing the program into computer system, and if the client dissents, she has the choice to return the packet product bundle. The Shrink-wrap contracts safeguards the item creator by clearing the maker of any encroachment of copyright laws or protected innovation privileges when the client tears the item or the covering for the merchandise. Notwithstanding, there is no fixed choice or point of reference in our country for the Shrink-wraps contract.

Click or web-wrap contracts:

A Click-wrap agreement alludes to an online agreement that needs endorsement or consent of the client through the "I Accept," or "Alright" button. With the click wrap arrangements, the client should acknowledge the circumstances before utilizing particular programming. Clients who disagree with the agreements will not be able to utilize or buy the item following crossing out or dismissal. Somebody almost consistently maintains web-wrap arrangements. Before the client consents to the terms of administration, they should be recorded. For instance, web-based shopping, programming download or establishment, to buy aircraft tickets or music web-based, utilizing sites, enlisting a record on an online media site, and so forth.

Browse-wrap contracts:

A Browse-wrap contract is an agreement that is restricting on at least 2 parties through the use of a site. In the case of a Browse-wrap contract, a common client of a specific site is expected to acknowledge the agreements of utilization as well as other site rules for proceeding with use. Such web contracts are exceptionally normal in our consistent routines. Different countries have managed such internet-based arrangements and verified that both Shrink-wrap contracts and Click-Wrap contracts are enforceable the same length as the agreement's overall standards are not violated.

E-signatures:

The parties have to first frame down the terms of the agreement to suit their inclinations, the phase of implementation by appending an online endorsement is the accompanying advance. The Information Technology Act 2000 perceives two sorts of marks:

- Computerized marks produced by digital signatures generated by an asymmetric crypto-system and hash function,
- Electronic signatures defined in its II schedule, wherein the user of an Aadhar card is assigned a UIN (Unique identification number) via which they can electronically sign and verifies documents via third-party forums (regularly through a validity of a one-time-secret key). The provisions of sec 5 of the Information Technology Act 2000 characterize E-signatures as a wide scope of means for marking an archive, though an advanced mark is a sort of virtual endorsement that utilizes cryptography.

While an absence of a law on the legitimate validity and achievability of E-signatures demonstrates that acknowledgment of similar remaining parts is unsure, endeavours have been incorporated to beat these drawbacks through modifications to the Information Technology Act 2000. The Information Technology (Amendment) Act of 2008 traded the expression 'advanced signature' for 'electronic mark' fully intent on widening the extent of virtual endorsements.

LEGAL CHALLENGES

Fundamentals of an E-contract:

- A deal prerequisite to be made
- The deal should be recognized
- There must be lawful thought
- There must be a goal to make legitimate relations
- The gatherings should have the option to contract
- There should be free and unaffected assent
- The object of the agreement should be legal
- There should be conviction and probability of execution.

Development of Online Contracts or Electronic Contracts:

Like a normal agreement, online agreements are enforceable e-arrangements comprising of a proposition and acknowledgment. An agreement can likewise be inferred from the lead of the gatherings like the trade of messages or tolerating a condition or terms or by downloading, and so on an assortment of strategies are accessible for framing electronic/online agreements:

Email: By trading email correspondences, the gatherings can make a substantial agreement. Offers and acknowledgments might be traded completely by email, or can be joined with paper records, faxes, and conversations.

Site Forms: In many cases, a web-based business Web website will make labor and products available for purchase, which the client orders by finishing and communicating a request structure shown on screen. When the seller acknowledges the request, an agreement is framed. The different varieties of Goods, products, and services may then be conveyed disconnected. The Terms of Use of a site would likewise turn into a legitimate agreement once the client acknowledges something similar by clicking "I Agree".

EULA: The End User License Agreements additionally structure substantial agreements where the end buyer clicks the "I Agree" or I Accept the Terms" button in the structure.

So, the significant distinction between an e-contract and a conventional agreement is that e-contract is paperless and the gatherings probably won't meet eye to eye. Here we are attempting to investigate and analyze various parts of a conventional agreement versus an internet-based agreement[1].

The legal validation of the Shrink Wrap contracts:

The legitimacy of the Shrink Wrap contracts came into question by the case ProCd Inc versus Zeidenberg[2]. For this situation, the producers of certain goods have entered a Shrink Wrap contract in its packaged software programming. The client bought the product however didn't follow the permit confining its business utilization. To authorize the permit, the litigant petitioned for a directive. The court denied the injunction while expressing that however the agreements are not unequivocally given, the permit was to be treated as a common agreement. Accordingly, it is enforceable.

The IT Act, 2000 specifically excludes the following documents from electronic transactions:

- Any Negotiable Instruments
- Power of Attorney
- Trust Deed
- Will
- Sale Deed or Conveyance deed concerning the immovable property of any documents relating to any interest in an immovable property.

TECHNICAL ISSUES

Technical Issues with tips to follow before using technology online:

- **Keep your computer always updated with the latest patches:**

Cybercriminals target personal information, such as mobile phone numbers, bank account numbers, emails, and passwords to take control of your computer, laptop, or tablet. They accomplish this by infecting your computers with harmful software or malware in the form of a virus. Maintain a clean of the history up-to-date system at all times, and never click on any strange, messages, notifications, emails, or any other links without any knowledge on it.

[1] IT Act 2000, Information Technology Act 2000, Bare Act, Information ...." http://www.itlaw.in/. Accessed 2 Jun. 2018

[2] *ProCD, Inc. v. Zeidenberg*, 86 F.3d 1447 (7th Cir. 1996)

- **Make sure your computer is configured securely:**

Our computer systems store a lot of sensitive information. Only for this purpose, the cybercriminals hack our computer systems. To safeguard this the only way is to secure your data with security of your data, take a few basic actions to maintain the security of your computer, such as connecting to a secure connection, installing antivirus, removing unwanted software, and securing your online browser.

- **Choose strong passwords and use the OTP method for safe better access:**

In this present digital era, we do a lot of activities with our computers, such as banking, paying bills online, shopping, and others, and we maintain our personal information in online for easy and quick access. Hackers mainly access to take control of our device into their control through a link to get access to our systems. If we use a strong password or OTP they will have a hard time cracking our passwords if they are long and complex. As a result, use complex passwords that include capital and lowercase letters, digits, and special characters and make your own OTP in this technical world for safe & better access.

- **Use certified software security to protect your computer:**

When you connect to the internet, your computer will be connected to millions network of with other people online. And you will be clicking with different links based on the purpose we use that if you're connected to such a large network, you're vulnerable to hackers, virus writers unknowingly. However, by installing appropriate security software with the reputation of brand security features especially for the internet to safeguard your PC online and keep your data safe from hackers.

- **Check your bank account, debit and credit card statements frequently:**

You should always frequently check your bank account, debit, and credit card accounts details to see if anything is wrong. If found any you will be able to take action on time if you do so such verifications frequently.

- **Try to avoid or Be very cautious while using public Wi-Fi hotspots:**

Using public Wi-Fi hotspots at Internet café, Railway Stations, Airports, Restaurants, hotels, shopping malls, and others are not recommended and not safe. Even if you believe they are secure to access there would be a possibility of hacking as you use their password, you are still sharing that platform with millions of other people. And strictly avoid sharing personal information, money transactions on such vulnerable platforms.

- **Avoid saving Personal information and share it online:**

Try to not communicate personal information such as your name, address, phone numbers, bank account, debit & credit card details, or any other financial information to anyone when using the internet. When purchasing online, ensure sure the websites are secure and verify with your system's privacy settings are enabled by using a firewall or antivirus software are updated and active.

- **Be conscious before you click on stranger messages or links:**

Try to avoid clicking on every link you receive through stranger messages, links, offers, or emails from different sources. Do not respond to everyone's offers that appear to you on the internet. Never provide information or respond to emails or offers that want personal information such as bank account numbers, credit card numbers, OTP, and any other information to personal or financial details to transfer in the name of JOB offer.

- **If you have any suspect, Block the number:**

If you receive any friend requests from unknown people or different number with your friend›s photo on your social media accounts such as Facebook, LinkedIn, and others, do not accept them till you cross-check with your friends and if not true just block it.

- **Use of multiple e-mail accounts:**

Using one account for everything is too risky and not safe all the way because if your account's password is cracked, the hackers will have complete access to your personal and financial information. If you have multiple e-mail accounts for your needs with different IDs over social media accounts, it would be always a smart idea.

- **Do not pay any attention to the notifications or pop-ups:**

While browsing the internet, you may come across different notifications, pop-ups, and other advertising and providing items that appear based on your previous history check to be true and good with a form of a survey-or in the form of offers and others.

- **Two-step verification methods:**

It's always not safe to use quick access in today's world but it is a good idea to have two-step verification to protect your apps, email, social media accounts, and cloud services. You will be asked to enter a verification number given to your phone through SMS along with your password to get access to your computer or any other internet area.

- **Shop online only with secured and trusted websites:**

While shopping online use only trusted and secured websites. It signifies that your browser should have a locked padlock or an unbroken key symbol with an IP address of the internet site that will change from "HTTP" to "HTTPS." It guarantees the site's protection.

- **Do not open unknown or unauthorized links:**

Trying to open stranger links Hackers entice people to click on suspicious sites by false promises like offers, job forms, and others. If you feel any suspect, it is better to not open it and share your personal and financial information with them.

- **Do not save bank account, debit, or credit cards information online:**

Sharing or saving bank account, debit, or credit cards information to your friends online or saving on a website is not secure or safe.

- **Change of passwords frequently is safe:**

Always change your PINs, passwords frequently to safeguard your personal and financial details from Hackers and others.

- **Protect your social medial accounts from permissions:**

Do not give all the permission to everyone to see your information from the unauthorized persons and give access to the trusted ones only, cross-check, verify before you accept them by all aspects.

CONCLUSION AND FUTURE IMPLICATION

The Laws related to Information Technology in India have progressed significantly since the establishment of the IT Act, 2000. Be that as it may, there exists vulnerabilities and disarray concerning numerous parts of an internet-based agreement, particularly on the prerequisites of mark and stepping. With the latest thing of demonetization and digitization, annihilating any vulnerabilities in the legitimacy of e-contracts is by all accounts the need of the day and we earnestly trust the Government would make fundamental strides in such manner.

The Laws of Information Technology in India has progressed significantly since the establishment of the IT Act, 2000. Be that as it may, there exists vulnerabilities and disarray concerning numerous parts of an internet-based agreement, particularly on the prerequisites of mark and stepping. With the latest thing of demonetization and digitization, annihilating any vulnerabilities in the legitimacy of e-contracts is by all accounts the need of the day and we earnestly trust the Government would make fundamental strides in such a manner.

This is relied upon to build the benefit and force of looking into organizations by offering unprecedented admittance to a web-based worldwide business community with an enormous number of clients and a wide scope of items and organizations. Nonetheless, with the electronic understanding, the postulation centres not around people who settle on choices on unequivocal exchanges, yet on how hazards should be organized in an automated domain. Along these lines, the paper is to give default guidelines to allotting a memo to a social occasion to stay away from any coercion and error in the arrangement.

The current pandemic situation has given ample opportunities to drive Indian markets headed for paperless and quicker types of contracts. Regardless, because the Information Technology Act 2000 explicitly expresses digital signatures and e-signs from Aadhaar are acceptable, foreign citizens who do not have digital signatures governed under their respective technology laws or e-signs from Aadhaar will be unable to give consent via e-sign. All through the present situation, the overall signatories can depend on the marking procedure available to them to lay out their legitimacy through proof, for example, email correspondence or the individual's transaction to distinguish the intention of the contract.

REFERENCES

1. ProCD, Inc. v. Zeidenberg | Casebriefs. https://www.casebriefs.com/blog/law/contracts/contracts-keyed-to-farnsworth/thebargaining-process/procd-inc-v-zeidenberg/.
2. Jain, Sankalp, Legality and Enforcement of Restrictive Covenants in India (November 20, 2020). Available at SSRN: https://ssrn.com/abstract=3901903 or http://dx.doi.org/10.2139/ssrn.3901903
3. Vijayakumaran, Adarsh and Vijayakumaran, Adarsh, Legally Blocked: The Evolution and Legality of Smart Contracts (Augst 21, 2019). Vijyakumaran, A. (2019) 'Legally Blocked: The Evolution and Legality of Smart Contracts', in Raizada, S. (Ed.) Advancement in Legal Research: Transdisciplinary Innovative Dimensions, New Delhi, K. V. Publishers Isbn No. 978-81-934484-4-1, Available at SSRN: https://ssrn.com/abstract=3481038 or http://dx.doi.org/10.2139/ssrn.3481038
4. Neha Saini, Dr. Arvind P. Bhanu, Operational Aspects of E-Contracts: A Critical Study, International Journal of Management, 11(5), 2020, pp. 1721-1734. http://iaeme.com/Home/issue/IJM?Volume=11&Issue=5
5. Alan Davidson, The Law of Electronic Commerce (Port Melbourne: Cambridge University Press), 73, (2009)
6. Information Technology Act, No. 21, 10A, 2000 (India)
7. Indian Contract Act, 1872, S. 2(a).

17

INTERNATIONAL INITIATIVES TO COMBAT CYBER CRIMES

KEYWORDS

CYBER CRIMES, UNCITRAL, EUROPEAN UNION, APEC, COMBATING CYBER CRIME, DATA HARVESTING, RANSOMWARE, CYBER TERRORISM

CHAPTER SEVENTEEN

INTERNATIONAL INITIATIVES TO COMBAT CYBER CRIMES

AUTHORS

MEERA S RAJAN, LL.M STUDENT (CORPORATE AND COMMERCIAL LAW), SCHOOL OF LAW, SHARDA UNIVERSITY, INDIA

DR RITU GAUTAM, ASSISTANT PROFESSOR, SCHOOL OF LAW, SHARDA UNIVERSITY, INDIA

ABSTRACT

Nowadays, many services are available over internet such as internet banking, shopping, ecommerce and other n number of services that are increasing in both number and size as the internet advents, so does cybercrimes. The effect of cybercrimes on the society is huge. The authorities are trying really hard to provide cyber security to both netizens and the states.

Combating and investigating cybercrimes successfully, is a complex task since the area of jurisdiction (ie: cyberspace) is a virtual territory. Then too the world leaders are coping with this challenge and are adopting the best practices in legislation, policies, procedures, international treaties and resources to put a stop to cybercrimes. These methods are revised on a regular basis since the cybercrimes are ever evolving with new technologies.

The following international organizations were established to provide guidance to defend cybercrimes.

1. UN and UNCITRAL (United Nations Commission on International Trade Law)
2. European Union
3. OECD
4. Council of Europe
5. International Chamber of Commerce
6. WIPO
7. APEC
8. G8(Group of Eight)

The research paper shall consist of how these international organizations have played an active role in propounding the fundamental principles on which states can frame/enact their legislations to regulate and govern the activities in the cyberspace. Also how these entities have made sure that the dispute settlement in cyberspace has some standardized method.

In brief the research shall be an analysis of the various international mechanisms and how productive they are in preventing the cybercrimes.

INTRODUCTION

Internet has grown to an extent that we humans cannot live without it even for a single day. Starting from breakfast recipes to bedtime routine we heavily rely on the internet, and the pandemic has taught us to run classes and work online. It is not wrong if we say that our worlds revolve around the cyberspace. It is mind blowing and scary at the same time.

As internet has provided new areas to explore, it has also birthed opportunities for cybercrimes. These crimes in cyberspace find ways to evolve rapidly with the growth of cyber world. It doesn't confine into hacking, data theft or virus attacks. A wide array of cybercrimes is confusing the authorities since the territory where the crime occurs is purely a virtual one and baffling to us.

Unlike any other statute, one nation cannot legislate an enactment against cybercrimes, without the aid and advice of other nations. The area of enforcement is the reason behind this dilemma. Since cyber-attacks know no border, the world leaders are together, joining forces to address the issues in cyber security. This is the reason why we require a paradigm shift in prevention of cybercrimes.

Nevertheless, we have several international entities which have and is still working as a barrier in preventing cybercrimes. In this research paper we will see how they have provided us with basic cyber security and protection that we enjoy now, and how these are updated on a regular basis to cope with the ever-mutating cyber-crimes. Also, this paper shows us how cyber law has nexus to international law.

CYBER-CRIMES

Cyber-crime is the act of illegal usage of computers and the internet. The place where the perpetrator acts or ought to act, or the place where the consequences of the perpetrator's action take place is called the cyberspace. The **mens rea** in the case of a cyber-crime comprises of two elements. Firstly, there must be intent to secure access to any program or data held in any computer, computer system or computer network. Secondly, the person must know at the time that he commits the **actus reus** that the access he intends to secure is unauthorised. The intent does not have to be directed at any particular program or data or at any program or data contained in a computer, computer system, or computer network. The aggrieved has the legal right to initiate both civil and criminal proceedings against the offender based on the nature of the offence.

The nuance in cybercrimes that we face today is mainly because of the unprecedented pandemic. **Malicious domains** are one of the new cybercrimes on the loose. There is a rise in registered domains which contain the domain name "corona", "corona virus", "covid", and "covid-19" etc. While some of these sites are genuine and informative, the cyber criminals are milking this opportunity to create websites just for the sake of spamming, phishing, scamming and spreading of malware. They are taking advantage of the whole pandemic and the widespread use of internet which it has created to cover their illegal activities.

Ransomwares existed earlier but has regained its notoriety in these difficult times, since the medical institutions are toiling at providing the best they can do, they are likely to pay the ransom the cybercriminals demand when their systems are compromised by the ransomware. According to the Interpol reports, there was a huge escalation in ransomware attacks in the first two weeks of April 2020.

Data harvesting malwares such as Remote Access Trojan, info stealers, spyware and banking Trojans are also on the rise when the global internet usage became higher than usual during the pandemic. They steal and access the personal data by luring the netizens by making them believe they are given information about the pandemic.

The act of **Cyber terrorism** include damage to the protected critical computer system that contain sensitive information of national interest. The cyber terrorists use encrypted emails to plan their activities and execute their propaganda by using a modern technology called '**steganography**', which can hide messages in beautiful pictures or cartoons.

The 2001 Parliament attack in India was planned by using steganography. The act of perpetrators of 26/11 at Mumbai also falls under the category of cyber terrorism.

INSTITUTIONS COMBATTING CYBER CRIMES

The International Law Commission adopted at its 48th session in 1996, the Draft Code of Crimes against Peace and Security of Mankind, and submitted it to the UN general assembly. This made a huge impact on ambit of international law that crimes in cyber world would come under its purview, whether or not they were punishable under the municipal laws.

- **UN and UNCITRAL**

The UN is an international and worldwide organisation which includes almost all the nations, which facilitates and encourages the collaboration in international law& security, economic development, social progress and solving conflicts of international extent. The UN Guidelines for Regulation of Computerised Personal Data Files, 1990 casts a duty on every member nation to ensure that information about persons should not be collected or processed in unfair or unlawful ways.

The personal data shall not be used or disclosed except with the consent of the person concerned. Appropriate measure should be taken to protect files against natural dangers (accidental loss or destruction) as well as human dangers (unauthorised access, compromise of data by viruses etc.)

During the 11th UN congress on the prevention of cyber-crimes in 2005, there was a workshop on measures to combat computer related crimes, which were concluded by giving the following recommendations.

1. The UN should assist member countries in combatting cyber-crimes.
2. Enhancing and encouraging international law enforcement collaboration.
3. Encouraging the member states to update their legislation and strengthen their cyber laws.

In the early 2000's the general assembly of the United Nations adopted the Model Law on E-Commerce adopted by the UN Commission on International Trade law. In 2010, proposal were made to adopt a 'Global Cyber Space Treaty' for ensuring cyber security by prevention of cyber-crimes. Unfortunately, the proposal was rejected by the UN since China, Russia and a number of developing countries failed to reach agreement with U.S, Canada, United Kingdom.

- **European Union**

The EU consists of 27 European nations. The member nations are working together in combatting cyber-crime and cyber terrorism. The organisation enhances cross border operation between member countries.

In January of 2001, the EU's Commission adopted statement on '*Creating a safe information society by improving the security of information infrastructures and combatting computer related crimes*. The European Union Directive requires that the member states shall provide that personal data must be:

a) Processed fairly and lawfully.
b) Collected for specified, explicit and legitimate purposes.
c) Adequate, relevant and not excessive in relation to the purpose for which they are collected and/

or processed.

d) Accurate and kept up to date.
e) Kept in a form which permits identification of data for no longer than is necessary for which the data were collected; except in the case of historical, statistical or scientific use.

- **Organization For Economic Co-Operation and Development (OECD)**

The OECD guidelines 1980 seek to ensure effective national measures for the protection of privacy and for international co-operation for the regulation of trans-national flow of personal data. These guidelines form the basis of legislation in many nations including India. The guidelines mandate that the international flow of personal data should be uninterrupted and secured.

The guidelines prescribed, many security measures or safeguards to protect personal data:[1]

a) Physical safeguards: Fire walls, anti-virus software etc.
b) Organisational safeguards: Authorised access to data, obligation for data processing personnel to maintain confidentiality.
c) Informational safeguards: Encryption, threat, monitoring of unusual practices and responses to them

These guidelines represent a significant step in the international protection of personal privacy. To implement these guidelines, all the member nations have enacted privacy laws and constituted authorities to enforce those laws.

In the early 2000's, these nations adopted another guideline "Cross Border Fraud Guidelines". These guidelines seek international co-operation to protect consumers against internet frauds.

In 2006, OECD adopted the "Recommendation on Cross-Border Co-Operation in the Enforcement of Laws against Spam, ("spam recommendation") which aims global co-operation against "spamming".

- **Council of Europe**

The member states of the council of Europe signed the Convention for the Protection of Individuals with regard to "Automatic Processing of Personal Data", in 1981 (Council of Europe Convention) with the idea of protecting the right of individual by protecting personal data. The Convention requires the State parties to take security measures for the protection of personal data stored in data files against accidental or unauthorized destruction or accidental loss as well as against unauthorized access alteration or dissemination.

- **ICC (International Chamber of Commerce)**

ICC mandates that while the states frame policies, active involvement of business parties and other stakehold-

[1] https://www.oecd.org/sti/ieconomy/digital-security/

ers must be sought. Such policy matters should cover issues relating to intellectual property rights, privacy rights, trade matters, security concerns, consumer protection and education.

- **World Intellectual Property Organisation (WIPO)**

WIPO has been instrumental in harmonizing copyright issue across many countries. The Copyright Treaty, 1996 and the Performance and Phonograms Treaty, 1996 are the two landmark treaties addressing intellectual property issues in the world.

The WIPO Copyright Treaty, 1996 is a special agreement under the Berne Convention, but not a party to WIPO Copyright Treaty. This treaty excludes ideas, business method and mathematical formulas. As per Article.4 of the treaty, computer programmes are protected as “literary works”. Article.5 of the treaty protects compilation of data or databases as intellectual property. The treaty provides exclusive right to the author and provides that the signatories shall establish enforcement teams to prevent infringements.

The WIPO Performances and Phonograms Treaty, 1996 aims to protect intellectual property rights of performers (including artists) and producers of phonograms. Many countries including India is still not a party to it. The treaty elucidates the moral and economic rights of the performers including rights of reproduction, distribution and commercial rental rights.

When it comes to the producers of phonograms, it grants rights of reproduction, rental, making available to the public and broadcasting. The treaty also provides for the right of remuneration to producers and performers.

CRITICISM OF WIPO

It failed to address the issues in cyberspace and hence failed to adopt adequate techno-legal measures to protect IPR in cyber space. There is absence of detailed provisions to deal with online copyright protection. The signatories of the WIPO treaties took no strict adoption and implementation of the provisions mentioned in it.

ICANN (Internet Corporation for Assigned Named and Numbers) policy

The WIPO established the online domain name dispute resolution system for domain name disputes commonly called ICANN policy. This process is not only quicker, but also cost effective. This policy was adopted in 1999.

Trademark holders can file cyber-squatting cases before the WIPO Arbitration and Mediation Centre. The registrar can cancel, suspend or transfer a domain name.

A party may choose one or three panellists from the panel of arbitrators, to decide their disputes. They decide through online means and the procedure takes 45 days to resolve the disputes.

The registrar transfers the domain name in question only if it receives an order from the court/arbitration entity deciding the dispute or receive instructions from the domain name holder. The burden of proof is with the complainant. He has to prove that:

1. Respondent's domain name is identical or confusingly similar to his trade mark or service mark.
2. Respondent has no legitimate interest or any rights with regard to the domain name.
3. It was a "bad faith registration".

In the case of NIIT Ltd vs Vanguard Design[2], defendant's domain name 'niitcrcs.com' was deceptively similar to that of the complainant. WIPO directed that the domain name be transferred to the complainant. They had to prove all these steps in-order to reclaim their domain name.

WORLD TRADE ORGANISATION

World trade organisation has contributed few things for the protection of cyber security through the TRIPS agreement. Article 10 of the TRIPS agreement protects computer programmes and 'databases' as copyrighted works. The following drawbacks of the Berne Convention and Paris Convention were rectified by the TRIPS agreement.

a) Failure to address many aspects of IPR protection online.
b) Lack of strategies for the enforcement and resolution of disputes imposition of trade sanctions.

The drawbacks of this agreement include:

It fails to address property issues like online name protection, blogging rights, royalty issues for digital music libraries, copy right over email accounts etc.

- Asia Pacific Economic Community (APEC)

The APEC privacy framework published in 2004 contains principles relating to protection of personal information, especially that places limitation on collection and use of personal data.

- G8(Group of Eight)

The G8 is a group of world's main industrial super powers. The G8 established 5 subgroups to employ and adopt the forty recommendations developed by G8. One of the G8's subgroups was the sub group on High-tech crime. They assist, advice and help the member countries in combatting cyber-crimes. It offers some recommendations to help its members to review their legislation to ensure that high-tech illegal acts are crimi-

[2] (2004) PTC (28) 98 (WIPO)

nalized by all member countries.

CONCLUSION

Combatting and investigating cyber-crimes successfully, is a complex task since the area of jurisdiction is vast and knows no boundary. There are international organisations which provide cyber security to the world. These nations have combined their forces and has made a few organisations with the idea in mind that they will prevent the rise of cyber-crimes with the evolving technology.

The organisations such as UN, EU, OECD, Council of Europe, International Chamber of Commerce, WIPO, APEC, G8 has played a crucial role in setting the rules in the cyber world. They made sure that there are standardised riles for dispute settlement.

REFERENCES

1. Gautam, R., Kulshrestha, P., & Goswami, M. A. K. (2021). Mediation And Family Dispute Resolution Mechanism: A Case Study On Clinical Legal Education. Elementary Education Online, 20(3), 2490-2490.
2. Gautam, R., "Proliferation of Cyber Crime and Indian legal system with special reference to Gwalior Division" Available at: https://shodhganga.inflibnet.ac.in/handle/10603/250817 Retrieved on: 22/07/2021
3. Pandey, N., Gautam, R., "property right of women in patriarchal indian society: a comprehensive study on legal narrative" Available at: https://www.researchgate.net/publication/361733554_PROPERTY_RIGHT_OF_WOMEN_IN_PATRIARCHAL_INDIAN_SOCIETY_A_COMPREHENSIVE_STUDY_ON_LEGAL_NARRATIVE_PROPERTY_RIGHT_OF_WOMEN_IN_PATRIARCHAL_INDIAN_SOCIETY_A_COMPREHENSIVE_STUDY_ON_LEGAL_NARRATIVE
4. Gautam, R., Medical health condition of prisoners and discrepancy in facilities among the states of Uttar Pradesh, Haryana and Delhi, International Journal of Health Sciences Follow journal, DOI: 10.53730/ijhs.v6nS6.12256
5. Gautam, R., Kanpur Philosophers ISSN 2348-8301 Vol IX, Issue V (IV), 2022151EFFICACY OF PROCEEDINGS OF CONCILIATION AND SETTLEMENT OF ANINDUSTRIAL DISPUTE UNDER INDUSTRIAL DISPUTES ACT, 1947, A CRITICAL Analysis. Available from: https://www.researchgate.net/publication/361733673_Kanpur_Philosophers_ISSN [accessed Sep 11 2022].
6. Gautam, Ritu, Cybercrimes and International legal regime, Available at: https://shodhganga.inflibnet.ac.in/bitstream/10603/250817/10/10_chapter-iv%20%20cybercrime%20issues%20and%20international%20legal%20regime.pdf
7. Gautam, Ritu, Cyber crime in India, Availablr at: http://hdl.handle.net/10603/250817

18

ARTIFICIAL INTELLIGENCE IN ADMINISTRATION OF JUSTICE IN INDIA: CHALLENGES AND OPPORTUNITIES

KEYWORDS

ARTIFICIAL INTELLIGENCE, HUMAN INTELLIGENCE, SPEEDY TRIAL, INVENTION AND DEVELOPMENT

CHAPTER EIGHTEEN

ARTIFICIAL INTELLIGENCE IN ADMINISTRATION OF JUSTICE IN INDIA: CHALLENGES AND OPPORTUNITIES

AUTHOR

MR. SANJEEV GHANGHASH, ASSISTANT PROFESSOR LAW, GALGOTIAS UNIVERSITY, GREATER NOIDA, UTTAR PRADESH, INDIA

ABSTRACT

In the era of advancing technological inventions and developments artificial intelligence so far has paved its way or marked its presence in a very cognizant manner. In India, where upon approximately 20000 judges handling over 30 million cases is hindering the speedy process of administration of Justice. It leads to denial of Justice to poor and under trial prisoners. With the manifestation of artificial intelligence in the workspace of judicial administration, it would let the cat out of the bag and would make the judicial system even more smooth and efficient fetching less of the burden to the officials. Artificial Intelligence Judicial system is more efficient, cost-effective and objective, moreover the role of judicial artificial intelligence might play a significant role in dealing with cases and transactional work. But Artificial Intelligence has its own limits too, as it is just a machine, and we cannot completely rely on it. As Human intelligence has

more ability to think out of box with their knowledge structure, application of mind and potential ability as compared to artificial intelligence which relies on the factual data, artifacts and algorithm. Bringing this technological change into limelight might serve as an impediment to the thinking ability of an individual as it would enhance more reliability over machines then our own psychological thinking skills. But, with both its pros and cons in consideration Artificial intelligence can serves as assistance in speeding up the judicial processes, maximising case handling efficiency and promoting Justice.

INTRODUCTION

People's jobs are being taken over by machines all across the world. Many people considered spell-checking and search algorithms to be "intelligent" information technology in the not-too-distant past. At our airports, face recognition is now frequently used to screen passengers. "The restaurant may be closed," Google Maps warns me as I approach my location. My laptop and phone respond to my inquiries with courteous voiced responses. The press frequently refers to 'robot' justice. There are assertions that computers will be able to precisely forecast court rulings and that we will no longer require human judges. We like to speculate about technologies that don't yet exist and how they should make our lives simpler. But, in reality, what do we understand about the usage of artificial intelligence?

Depending on the latest level of knowledge, this article examines the possibilities and hazards of AI technology in the courts. The paper's key points are:

1. how can machine learning be beneficial for lawyers and tribunals, and
2. what is required for artificial intelligence to be useful. Many court matters may be automatically processed, at least to some extent, and do not always require a complicated, custom-made strategy to judgement call.

As a result, the implementation of information technology, particularly artificial intelligence, varies depending on the situation. Which type of artificial intelligence has been already demonstrated to be effective in these many processes? How can artificial intelligence assist courts and judicial officers?

By concentrating on the three key steps of getting machine learning (the much more common subgroup of Intelligent systems) to "implement data, model, and application stage—this article presents a paradigm for comprehending the consequences of AI. In brief, I'm interested in the constraints and hazards that come with data-driven judgments in general, and in particular in the Indian context. This study's scope and methodology are important for three reasons".[1]

For starters, it represents an option to existing policy methods to tackle social and ethical difficulties, which are now categorized as challenges to adoption. The current strategy would be both short-sighted and ineffective.

[1] Jain, P., 2018. Artificial Intelligence for sustainable and effective justice delivery in India. *OIDA International Journal of Sustainable Development*, *11*(06), pp.63-70.

In cultures that are chaotic, prejudiced, uneven, and rooted in historical unfairness and inequality, AI applications function. The bedrock on which these technologies are created is inherently insecure if these vital social realities are treated as afterthoughts, add-on features, or even defects to be addressed. I illustrate the social and moral factors that must be taken into account while developing AI systems and policies, as well as providing a framework for doing so.

Second, it encourages a multidisciplinary debate on AI policies in India. So far, facilitating a discourse based on common language and comprehension amongst stakeholders and throughout sectors has been a major problem in this arena. By presenting this paradigm, I hope to express policy problems in modern terminology and conversely.[2]

Finally, it broadens worldwide debates on AI, ethics, politics, and legislation, which are now mostly based on Western perspectives. "Today's AI systems are considerably more than basic mathematical problems: they include socio-technical processes that are dependent on the environment in which it operates". For a variety of reasons, India is an essential jurisdiction to examine. It is a powerful force due to its massive size and developing AI sector.

ARTIFICIAL INTELLIGENCE

The word 'AI' can be interpreted in a variety of ways. Given the difficulty in defining terminology in this field, "I will explain a few technical languages in this section and describe their intended meaning within the context of this paper".

— A collection of "encoded techniques for changing data input into expected outcome, depending on specified computations" is referred to as an algorithm. It's a methodical, step-by-step technique that doesn't rely on human intuition or guessing.

— Artificial intelligence (AI) is the ability of machines to behave intelligently. Machine learning is perhaps the most effective and commonly used subset of AI approaches today, demonstrating a system's capacity to improve task performance and efficiency.

Because the Indian government places a high priority on developing technologies in the digital economy, "AI policy will change and grow quickly in the next few years". Aadhaar, the world's biggest integrated automated fingerprint identification project, is based in the nation and, based on how it will be utilized, can serve as a central focus for AI applications. "India is now at a key juncture in the creation of data privacy legislation, that will have a significant impact on how AI can and will work in the country".

While the introduction describes the problem that this article aims to solve, the following part will go through the article's intended scope and provide definitions and conceptual clarifications for technical terms used in the

[2] Pandey, S. and Shankar, U., 2021. Transforming the Justice Delivery System in India through Innovation and Technology: Opportunities and Limitations of Integrating Technology in the Judicial System., *27*, pp.123-158.

paper.

It will analyse the existing status of India's AI policy regime before leading the reader thru every stage of the paradigm, with the goal of providing background information for working through the conceptual methodology. Lastly, this approach has been applied to sectors now under consideration in India's policy-making procedures. Conclusions and thoughts will be included at the end of the paper.

Artificial intelligence is becoming a subject of discussion

The Indian government has placed AI development, adoption, and promotion at the top of its priority list, based on the belief that AI has the tendency to make people's lives simpler and society more equitable. "The Union government contributed significant financing to research, development, and skilling in new technologies such as AI in 2018, a jump of 100 percent over prior investments".[3]

This emphasis on digital technologies is nothing new. The Digital India program of the Union government aims to convert India into a "fully digitized society and knowledge - based economy". Digital India envisions delivering infrastructural facilities as a basic service to all citizens, including such digitalization into governance, and eventually empowering citizens.

The work of the Task Force aims to give insight on the path in which India's AI strategy should grow. Its primary strength is its concentration on accessibility technologies. However, a superficial (at most) ethical and social examination of India's AI ecosystem reveals the absence of legal, governmental, and civil society participation in this process.[4]

INFORMATION TECHNOLOGY AND THE COURTS: THE CHALLENGES

Delivering justice in particular instances is one aspect of enforcing the law, but the court also has a shadow duty in presenting norms to society as a whole. "However, courts and judges handle information immediately of the subject material; parties present the information to the courtroom, modifications occur during the procedure, and the conclusion is likewise information. This information processing isn't all about complicated customisation. Many matters require a basic evaluation without the need for a hearing, as well as some matters are resolved. Default judgments and declarations of inadmissibility are frequently issued. Complex, conflicting matters make up a small percentage of the cases which the judiciary will have to deal with". It cannot be overstated how important the method is. As a result, the requirement for information technology varies depending on the situation.

[3] LUOMA, SANNA. "Artificial Intelligence Improving the Delivery of Justice and How Courts Operate." *How Will AI Shape the Future of Law?* (2018): 63.

[4] Nandi, Anulekha. "Artificial intelligence in education in India: questioning justice and inclusion." (2019): 140-144.

The way cases are handled in administration and civil matters (particularly smaller magnitude disputes court proceedings) is largely determined by

1. the intricacy of the information in the matter and
2. the dependability of the result.

The outcome of a vast percentage of routine instances is predictable. In some circumstances, the court judgement is a document generated by a mainly automated process using data provided by the parties. The judgment document specifies an enforcement title. The court usually accepts digital filings wherein the file party submits data digitally so that it does not have to be manually re-entered.[5]

"Also, there is a considerable number of routine proceedings in family and work concerns. In this case, the judge performs a similar job to those of a civil-law registrar in determining the legal legitimacy of a proposed agreement between the parties". This might be a traditional divorce in India, but it can also be a parenting authority clause or the cessation of a contract of employment. The decision is, once again, a mainly mechanically written document affirming that the proposed solution is legal. "Digital file and workflow automation are by far the most important information technology requirements here, as well. Furthermore, a smart filing site can assist the parties in bringing their matter to court in the most efficient manner feasible".

The Judicial Courts handles ordinary matters inside the criminal justice process, and only those matters that require a decision are presented before a court. There is indeed a broad array of scenarios here as well, from the simple to the exceedingly complicated. In all complex cases where the judge or panel must render a decision in order to bring a case to a conclusion, information technology is primarily required in the form of cutting-edge systems and make legal sources readily available, as well as a digital court document that can present huge volumes of information in an adequate way. Because artificial intelligence is indeed a sort of information technology, it may be used in a variety of situations.[6]

What role does artificial intelligence play in the legal system?

"AI may be applied in a variety of ways to address a variety of needs. There is a lot of sales hype about AI for courts. It has been stated that this would make it much more impartial, and also that AI, unlike human judiciary, does not grow weary or rely on glucose concentrations to operate. That is largely conjecture. However, the discussion here focuses primarily on what we currently understand based on data". Its concentration is on tried-and-true technology, like artificial intelligence (AI) that has already shown to be helpful in practice. Are robots, on the other hand, capable of judging? On this one, the judgment is still out.

[5] Kalyanakrishnan, Shivaram, Rahul Alex Panicker, Sarayu Natarajan, and Shreya Rao. "Opportunities and challenges for artificial intelligence in India." In *Proceedings of the 2018 AAAI/ACM conference on AI, Ethics, and Society*, pp. 164-170. 2018.

[6] Nandi, Anulekha. "Artificial intelligence in education in India: questioning justice and inclusion." (2019): 140-144.

1. Putting information in order.

Pattern recognition in text files and documents can be beneficial, for instance, "while sorting huge numbers of instances or in complicated situations with a lot of data. eDiscovery, an automated inquiry of electronic material for disclosure well before the beginning of a court proceeding, is an illustration from the United States of America. eDiscovery makes the performance of machine intelligence AI, which develops the optimal method for extracting the important sections from a vast quantity of data through learning. The search keywords and code are agreed upon by both parties".[7]

The judge evaluates and approves the deal. The judges in the United States and the United Kingdom have recognized this approach of document analysis. Manual file research is slower and less accurate than this procedure.

2. Give advice

Individuals and prospective parties to a legal case who are seeking a resolution to their issue but don't know what they'll do might benefit from AI that can counsel them. Legal practitioners can benefit from advisory AI as well. AI not only searches for appropriate data, but also offers a response to a query. The user must next determine whether or not to follow the recommendations. This advisory position can assist individuals in resolving much more of their difficulties on their own, avoiding disagreements and court proceedings.

If advise isn't enough, assistance in coming up with a solution also is an option. Assisting with the formulation of a remedy that involves court scrutiny, such as a petition or a summons, might make the judge's decision more regular.

3. Prognoses.

Artificial intelligence (AI) that promises to really be capable of predicting court rulings has sparked a lot of curiosity. Predictive justice is the common English/American name for this. Because the output of the forecasting models is neither just nor predictable, this word has sparked debate. Forecasting is a much more accurate phrase that reflects current disputes. The result appears to be more akin to a weather report than a proven truth. Court processes, like the weather, have an unpredictably unexpected conclusion.

That danger grows as more knowledge and concerns become available. One of the reasons for the high interest in AI is that it promises to be able to minimize risk. Different commercial forecasting techniques are available in the United States. "As a result, their inner workings are kept a trade secret, and

[7] Reiling, A.. (2020). Courts and Artificial Intelligence. International Journal for Court Administration. 11. 10.36745/ijca.343.

we have no idea how they operate. However, certain non-commercial applications have been developed, and we have some knowledge of how they work".[8]

FUNDAMENTAL RIGHTS MUST BE RESPECTED

1. Ensure that "AI applications and technologies" are designed and implemented in a way that respects fundamental rights including privacy, equitable treatment, as well as a fair hearing.
2. Treatment on an equal footing. "Discrimination between people and groups of persons should be avoided. COMPAS's experience demonstrates that discrimination and unjustifiable distinctions between persons and groups are a serious danger. The algorithm's data might be the reason, and prejudice could be built into the algorithm altogether'.
3. Data protection. Verified resources and information that cannot be tampered with should be utilized when processing court judgments and data, together with transdisciplinary models in a secured technological landscape.
4. Transparency. "External audits should indeed be authorized, and data processing procedures should be made accessible and understandable".

JUDICIAL GRID IN INDIA FOR AI (THE OPPORTUNITIES)

It is well known that now the Indian judicial system has a large caseload to deal with. According to research published in September 2021, India's high courts have 5.8 million unresolved cases, despite having disposed of around 1.8 million new cases per year on average during 2015 and 2019. Because new-age technologies like "AI, Nlp, and Ml" have permeated practically every industry, their application in law and order might be extremely beneficial in enhancing our court system. In India, the groundwork for accepting these technologies has already been laid.[9]

"The SUPACE (Supreme Court Portal for Assistance in Courts Efficiency)" was launched this year. Machine learning is used to cope with vast amounts of case data. SUPACE, according to Bobde, will be a hybrid of humans and machines that will not be utilized for decision-making. Data gathering and analysis will become the emphasis of AI systems.

[8] Chandra, Geetanjali, Ruchika Gupta, and Nidhi Agarwal. "Role of artificial intelligence in transforming the justice delivery system in covid-19 pandemic." *Chandra, G., Gupta, R. and Agarwal* 2020 (2020): 344-350.

[9] Jain, Parth. "Artificial Intelligence for sustainable and effective justice delivery in India." *OIDA International Journal of Sustainable Development* 11, no. 06 (2018): 63-70.

COURTS IN THE DIGITAL AGE

The Indian administration already has established e-courts, but their reach must be expanded further to address the number of cases we are now dealing with. The Judicial Branch and Constitutional Court were allowed to operate online during the COVID-19 epidemic. Electronic courts provide a more time-saving and efficient justice-serving platform with improved case and courtroom management capabilities. Because information can be received digitally, the odds of important statements, data, or proof being misplaced will be considerably decreased. Online procedures can be used to record evidence from eyewitnesses who are unable to be there in person.

ALREADY IN FULL OPERATION THROUGHOUT THE WORLD

AI and big information analytics have found their way into the law-and-order sphere. Promethea is an artificial intelligence tool developed in Argentina by the Innovation and Artificial Intelligence Laboratory of the University of Buenos Aires School of Law and the Buenos Aires Public Prosecutor's Office. Its goal is to expedite bureaucratic hurdles so that more time may be spent on difficult case analysis. It can also find urgent instances in enormous amounts of data in under two minutes.[10]

AI has also been used in the delivery of justice in Brazil. It conducts preliminary case analysis using an AI program called "VICTOR" to lessen the court's workload. The Brazilian Supreme Court uses it.

UNESCO is also providing online training on AI as well as the Rule of Law for judicial officers. The training will encourage a participatory discourse with judicial operators about AI-related developments in the legal system and court judgements on artificial intelligence, according to the statement. It undertook a poll of judicial operators throughout the world to better grasp the difficulties at hand. The poll gathered 1265 replies from judicial practitioners in 100 countries, in multiple languages.

CONCLUSION

The major focal areas are ethics and privacy. If used ethically, AI can be a powerful instrument in the administration of justice. Another area in which policymakers must exercise extreme caution is data security and the avoidance of critical information breaches. If the lawmakers can fix these issues and develop new legislation.

What does AI have to offer in terms of fairness, but what does it require? This article looked into what is understood about AI in the legal system. Because not all judicial work involves complicated bespoke work, the necessity for information technology varies from case to case. AI, which really is, after all, information technology, may thus be beneficial in a variety of ways for a variety of situations. Some AI continues to show its worth in the real world. There is currently no proof that robots will be able to judge. More structure and significance

[10] ESCAP, UN. "Artificial Intelligence in the delivery of public services." (2019).

should be added to legal information. For the time being, explaining how the outcome was achieved using AI is not possible. People, litigants, and courts can already use AI to organize information.

Similarly, in India, judicial duties that can be hastened via the employment of intelligent technology can be discovered. These activities might range from simple things like function is to allow to more difficult ones like evidence assessment. This would not only save the courts time, resulting in better use of public funds, but it may also help to reduce the influence of the judge's personal prejudices in decision-making. Of course, no technology, no matter how sophisticated, could ever substitute a human judge. Nonetheless, they may aid judges in their decision-making by providing considered and unbiased assessments, guaranteeing that justice is not jeopardized in the method of negotiating with a high number of cases.

Artificial Intelligence already has proven its worth in a variety of fields, including medicine by providing treatment during surgeries, logistics in the method of self-automobiles, advertising by monitoring consumer buying behaviour, and so on. It will undoubtedly be a boon to ensure a long-term and efficient justice system. As a result, using Artificial Intelligence in judicial decision-making is a realistic strategy for reducing case pending times not just in India as well as in other jurisdictions, as well as assuring efficient and long-term traditional justice systems around the world.

19

CYBERSECURITY AND SUSTAINABLE DEVELOPMENT

KEYWORDS

SUSTAINABLE DEVELOPMENT GOALS (SDG), CYBERSECURITY, TRUST, INFORMATION COMMUNICATION TECHNOLOGY (ICT)

CHAPTER NINETEEN

CYBERSECURITY AND SUSTAINABLE DEVELOPMENT

AUTHORS

NIKITA DEO, RESEARCH SCHOLAR, MANAV RACHANA UNIVERSITY

PROF ANITA SINGH, PROFESSOR, SCHOOL OF LAW, SHARDA UNIVERSITY, INDIA

ABSTRACT

Sustainability and Cyber security are essential to gain the competitive edge in the firms and development of overall economies. This needs to develop Trust in Information and Communication Technology (ICT). Keeping in view the current trends in technological, ethical, economic and legal environment, Trust is considered to be crucial for business and it fosters both sustainability and cyber security. It is pertinent for the Government and business firms to create a balance between the latest technologies and adoption of the stress –tested technology without hastening to be the earliest adopters of new technologies. Research suggests the socio-economic importance of trust in security of digital environment considering the Sustainable Development Goal (SDG). It is very pertinent to understand the mechanism for the effective use of innovative technologies for the realisation of the Sustainable Development Goal (SDG), and also how to track them. In the absence of effective cybersecurity practices, the organisation would substantially undermine the financial and reputational costs of cyberattacks.

The purpose of the research is to explore elements of sustainable management

into cyber security that would help in reframing the perceptions of cybersecurity from fear, uncertainty and a doubt to a more proactive mind-set of opportunity, dynamism and transformation.

The emphasis of this paper is to conceptualise the balance between sustainable development goal and cyber-security. Analytical research methodology will be adopted to understand the concepts, opinions or experiences.

INTRODUCTION

During COVID-19 more than two billion people were connected through internet and more than 60 billion Google searches in a month and approximately every minute 156 million emails were sent. Pandemic has increased the dependence of individuals and professionals on digital technologies and has resulted in increased surveillance. The internet enabled devices are vital and have become hallmark of social life. This dependence on technology affects people, organisations, and functioning of administration and the Government. This socio-technological phenomenon has both political and societal implications, and its impact is uncertain. Now a day's data breach and malicious attacks continue to damage companies and organisations bottom lines.

UNDERSTANDING CYBER SECURITY

In general, cyber security refers to the techniques of protecting computers, networks, programs and data from unauthorized access or attacks that are aimed for exploitation. Scope of cyber security includes Application Security, Information Security, Disaster Recovery and Network Security.

Basic Application security such as Session Management, use and role of Authentication & Authorisation, Parameter Manipulation, Auditing and Logging etc. ensures the measures to be taken to protect applications from the threats during the life –cycle development.

Information security protects the information from unauthorized access. The techniques that are used to protect the privacy are authentication & authorisation of user and Cryptography.

Disaster recovery helps in resuming the normal business operations after a disaster. It includes the process of establishing priorities, developing recovery strategies and performance risk assessment.

Network Security ensures protection of the usability, reliability, integrity and safety of the network. It identifies the various problems and restrict them from disseminating in the network. Anti-virus and anti-spyware, Firewall to block unauthorized access to the network, Intrusion prevention systems (IPS) to identify fast- spreading threats such as zero day or zero-hour attacks and Virtual Private Networks to provide secure remote access are the components of Network Security.

SUSTAINABLE DEVELOPMENT

Brundt land Commission in its report "Our Common Future" (1987) defined "*Sustainable Development is the development that meets the needs of the present generation without compromising with the needs of future generations*." Its objective is to develop a comprehensive, sustainable, and flexible ecosystem for the people and the planet. The main features of SDG are to increase per capita income, judicious use of natural resources, and preserving the resources for future generations.

In order to tackle the crisis of global environment such as overheating, climate emergency, and ozone layer consumption , United Nations 2030 Agenda adopted 17 Sustainable Development Goals (SDG) and 169 targets as part. These goals include eradicating poverty, hunger, ensuring food security, promote healthy lives, equitable quality education and lifelong learning opportunities, ensure gender equality, availability and sustainable management of water and sanitation. It guarantees access to affordable, reliable, sustainable, modern energy, sustainable economic growth, employment, building sound infrastructure, promote sustainable industrialization, fostering innovation, reduce inequalities among the countries, safe, resilient and sustainable cities and human settlements, promote sustainable use of oceans, marine resources, protect, restore, and promote sustainable use of ecosystems, halt biodiversity loss, etc.

IMPACT OF CYBER SECURITY AND SUSTAINABLE DEVELOPMENT

ICTs (Information and Communication Technologies) and Technology plays an important role in education, developing sustainable cities, maintaining clean energy, developing resilient infrastructure, promoting sustainable industrialisation, encouraging innovation. It's very critical to effectively provide the safety, security and resilience within cyberspace for technology.

Cybersecurity is considered as a component which helps in realizing and maintaining the general ICT (Information and Communication Technology) security objectives of availability, confidentiality and integrity. According to CTO (Chief Technology Officer), Every country requires to adapt an effective Cybersecurity Strategy to captivate the increasing cyber-dependant trade and commerce. A strong cybersecurity framework helps in realising the prospects of the cyberspace, without having any fear or reluctance to individuals, companies and nations and it promotes cross-border delivery of services and free flow of labour.

A country's preparedness to respond to the challenges of cyberspace is enhanced by cybersecurity framework. Measures like economic development and attraction of international business strengthens and protects the critical information infrastructure. Poor cybersecurity is considered as a hindrance to the development and trust in ICTs (Information and Communication Technologies) and results in lack of trust in online systems and services. Lack of an effective cyber hygiene leads to susceptible increase in cyber-attacks that promotes a lack of trust in the digital economy. The topic of sustainability is unmissable at the moment. As the urgency of the situation grows, it continues to demand attention from various sectors and industries within society. It is sometimes difficult to understand where the cyber security industry fits in the world. Whilst traditionally from very different worlds, they are united through the characteristics of constant innovation and the capacity to bring about real change for the better. Certainly, cyber security has a bigger role to play in the overarching battle for a more sustainable world than one may initially think.

CYBER SECURITY TOWARDS SUSTAINABLE DEVELOPMENT GOALS

- The economic growth is supported by enhancing the awareness of the benefits of digitization and promoting trust in it.
- The eradication of the poverty depends on individual's capacity to examine information over the Internet and that can be hindered by unauthorised access to information services and the unprotected networks.
- ICT (Information and Communication Technology) helps in a stable food supply and distribution mechanisms during famine. Digitization in the healthcare sector capitulates immediate dividends, but it also endangers data of the patient to new risks and makes hospitals and other service providers vulnerable to new risk.
- ICT (Information and Communication Technology) allows wide distribution and easy delivery of educational products and also safeguards the privacy of students. It is strictly required to be equipped with important skills while using computers and digital technologies which are required for good practices.
- Research suggests that inequalities in cybersecurity leads societal inequalities, research on gender lines is still negligible on the topic. It is very pertinent to have sound online resources for reporting prejudice and brutality against women to avoid the risk putting women at further risk.
- Cybersecurity is also important for the protection of pivotal systems that use IT (Information Technology). There are evidences of various hacks on pivotal infrastructure, energy grids, water and sanitation systems.
- Automation and automated systems are increasingly required for affordable and clean energy.
- The growth of the economy largely hangs on factors like money stuck in the bank, ensuring the control of intellectual property, and the availability of procedures for business use.
- Payment systems from mobile are playing a critical role for distributed access to financial flows and it again needs to exhibit the secure payment systems leading to economic growth.
- Increasing access to ICT (Information and Communication Technology) and new internet-connected technologies needs to manage the risk of usage of ineffective technologies security.
- Protection of the integrity of individual's information should be at precedence irrespective of their status in the society, it should be equitable and should not vary whether they are the poor, rich or powerful.
- Smart cities having attributes like intelligent tangible, social, institutional, and economical structure leads to substantial sustainability. The challenges due to increased reliance on apps contributes to issues around internet bandwidth surface and risk of cyber-attacks cannot be denied.
- It is important to ensure and protect the fundamental freedoms of public admittance to information in conformance with national codification and international agreements.
- With the help of international cooperation relevant national institutions should be strengthened

through, institutional building at all levels, especially in developing nations, and measures to be taken to counter terrorism and prevent violence and crime.

- Information systems has enhanced transparency and has strengthened the delivery of justice.
- To safeguard the interest of the population from the organized criminal groups engaged in the cyber-crime due to low barriers, the police should be empowered to identify and prosecute cybercrime.

ISSUES AND CHALLENGES OF CYBER SECURITY

Professionals and the organisations face many common issues which are:

1. *Recognition of Target*

Organizations assets and data attracts cyber criminals. According to Matthew Eshleman, CTO (Chief Technology Officer) of Community Information Technology Innovators, most companies have things in the modern economy that attackers require which includes information and money and organizations of every size face cyber threats.

It is important to have a basic knowledge of best practices in cyber security in order to have a right path for majority of the companies. *Kevin Raske, a cyber-security marketing specialist at Vipre* is of the opinion that one should be always aware that they are a target. The cause of the most of the breaches are confined to human error so it is required to develop a defense by acknowledging that the attackers might target the company.

2. *Lack of threat awareness among employees*

Steve Tcherchian, CISO (Chief Information Security Officer) and chief product officer at XYPRO, observed that the employees are often the weakest link in any cybersecurity program. According to him one can spend the entire money as one requires on antivirus, and other protective filters and technologies, but if employees are not educated and trained to identify the risk and scams and are not able to activate the innate immune system to overcome the basic threats such as phishing and malware by the organizations, the whole investment is useless. Employee awareness cannot be configured without follow ups and continuous training, feedback and follow-ups are required.

According to Ron Harris, vice president of Omega Computer Services, remote work has led to worsening of this issue. He said that most of the employees experienced work from home for the first time and they were simply not aware how to protect and to avert cyber-attacks like ransomware and the worst part is that there were helpless as there was nobody around to help them and they were not able to identify whether the email received is lawful or website is guarded to download a file from it. Harris suggested it should be made clear by the companies to its employees that where they should forward the suspicious email to the Information Technology department. This may reduce and prevent the issues of ransomware, or risk of cyber-attacks.

3. *Breach of Data due to remote work*

Magda Chelly, founder of Responsible Cyber expressed that with majority of the employees working from home resulted in likelihood of breaches from hackers which is called as a parameter-less environment. In these situations, there is a possibility of connections to other networks with non-approved equipment. Further he suggested that there may be no parity at enterprise-level security which provides security measures and controls and the technology in place. Zero-trust strategies in the companies, has encouraged the cyber security professionals to adapt perimeter-less concept.

Zero Trust strategies is applicable in many organizations it, require all the users irrespective of any level, to validate the authorization before getting hold to the key areas of the network

4. *Crypto viral extortion*

This type of virus conceals files on a device, making them remote or inaccessible and un usable is known as Ransomware or crypto viral extortion**.** In this the attackers ask for a ransom in in lieu of decryption of corrupted files. Sometimes the attacker threatens the person or the company to expose or leak the information when the ransom is opposed, which is usually desired in cryptocurrency.

According to Ian L. Paterson, CEO of Plurilock, due to unawareness among employees regarding the threats, there is attack on sharing and misusing the company's data and employee credentials in every 11 seconds. The credentials are compromised due to lack of multifactor authentication which has not been globally permeated till date. The organization is facing the challenge at both human as well as technology end.

5. *Absence of security patches*

According to *Courtney Jackson, Chief Executive Officer (CEO) and cyber security expert at Paragon Cyber Solutions LLC (Limited Liability Company),* during the process of the vulnerability assessments done by him in various organizations it was identified that out of the 100 plus, in majority of them security patches were lost from their device like user workstations and laptops. It is a matter of concern as the use of these security patches are vital to communicate the vulnerability discovered in the product of the companies. If the installation of the security patches is not done on priority the organizations assets are put at loss.

6. Policy to Bring Your Own Device (BYOD)

The policy of companies to use your own device by the employees at the workplace or remotely working has enhanced the risk that a BYOD environment can bring into the company. Though the aim is to make things easier but the threats which can be encountered cannot be ignored. The organization should follow few common steps to protect disturbance caused by COVID-19. It has escalated security issues in BYOD threats. Role-based, two-factor authentication and network access control are a few measures are used to continuously ensure the data are updated. According to *Andrew Douthwaite, CTO (Chief Technology Officer) at* Virtual Armour ,the organization needs strong employee passwords and exit process having mechanism to clear the devices of ex-employee and protect the data.

7. Contingency Plan

Marius Nel, CEO of 360 Smart Networks opined, most of the companies do not pay attention to cyber security measures, they depend on the systems or services for data safety. In the absence of any back up or contingency plan there is always a risk of cyber-attacks that can have disastrous impact on companies and the organisations. It was observed in the case of Baltimore City ransomware attack all the mission-critical data was not supported and due to this negligence, the data was lost forever.

8. Need for formal corporate security program

Irrespective of the size company should have a formal corporate security program having a sound security policy with acceptable use, prompt response and physical security. But most of the companies lack this proactive approach. The mangers should understand that the absence of effective security program put the business at a high risk of an attack and loss of information.

9. Handling Cybersecurity issues

It has been observed generally business leaders consider cyber security as an Information Technology (IT) issue**.** Douthwaite, views cyber security attacks as financial issue of the organization, it is suggested that the average cost of breach of the information is approximately $4 million so treating cyber security issues should be a way of life for the organizations. The core is that strategic thinking and continuous tactical actions are required to mitigate the business risk. The most effective and economical way to protect the business from the risk is to provide training to the employees in basic cyber security.

10. Unawareness of Information Security among the Board Members

Board members of the companies are concerned with the understanding of company's policy and business processes they are not interested in understanding the issues of information technology. The IT department may have a robust proactive plan for the information security but in the absence of support from the board members, they never get the resources because they are not able to understand cyber threats **(***Braden Perry, cyber security attorney with Kennyhertz Perry, LLC (Limited Liability Company).*

It is vital for the board members to understand the issues of cyber security and take proper care in recruiting IT or cyber security professional who is experienced and can mediate to interpret the IT language into business and vice versa. The cyber issues should be resolved with better communication between the leaders and IT department while investigating the cyber issues.

11. Need for trained Cyber security professionals

Cyber security issues of an organization can be resolved by hiring or consulting a strong trained security professional. Though cyber security personnel supply is less in the market but the measures should be taken by the organization to train the employees in the IT department who are dedicated to this field.

CONCLUSION AND FUTURE IMPLICATION

In today's technology driven economies, the issues of Cybersecurity have come to be a great concern area. The reason underlying this, the companies are more dependent on machines than their manpower and that is leading towards the increase in the cybercrime. The cyber breach can be the cause for dangerous environmental disasters endangering the innocent lives. It is very pertinent to provide a safe and sustainable environment for online cyberspace users. In this era of rapid increase in the usage of technology and its implementation it is very pertinent to adapt security countermeasures to prevent the system from cyber threats whether it is direct or indirect. It is a great challenge to identify, characterise and classify the threats and also to identify the sources that are required for a sustainable cyber –ecosystem

It has been observed that individuals who are indulged in the world of technology and internet are getting ready and preparing themselves to face the cyber risks by enhancing their own cyber military and cyber weapons. After land, sea, air and space now Cyber War has taken the fifth dimension of war. This war is very critical to the information infrastructure of the countries and they would lead to a devastating impact on the organisation. Organisations are facing various challenges with cyber security problems that has a devastating impact on the basic security characteristics of integrity, accessibility, and secretiveness, leading to disruptions and delay in the work processes and services. It creates a huge depreciation and overall scepticism in electronic transactions.

Every day unidentified Cyber-attacks are evolving that needs a lot of alertness and usage of effective measures to combat with the risk and keep the data and system protected. For an effective approach measure should not only be restricted to technical, but it should also take into consideration legal and regulatory framework. It is required to include measures for:

1. Requisite laws;
2. Essential legal or industry standards;
3. Announced public service and awareness-raising programs
4. Skills development programs;
5. Propagating best practices;
6. Inception of specialized agencies; and
7. Adequate international law enforcement cooperation.

In this current era, the entire world is facing Cybercrime, Cyber bullying, Cyber war, Cyber terrorism and many such anti-social issues that have gained a lot of attention. We must all together contribute our efforts to disseminate and propagate peace by taking proactive cyber security measures and also introducing peace into the cyber ecosystem.

The UN (United Nations) in 2015, found 17 Sustainable Development Goals (SDGs) and targeted to achieve it by 2030 – starting from removing poverty and undertaking stability and peace to fight discrimination and climate change. Digital technologies, mainly the internet of things and artificial intelligence (AI), can lead to putting efforts to achieve the SDGs (Sustainable Development Goals). For example, with the help of Artificial Intelligence one can help detect malnutrition using photographs of individuals living in a given area. The adoption of ICT (Information and Communication Technology) is continuously changing every aspect of our lives virtually. ICT (Information and Communication Technology) and connectivity can lead to productivity, innovation, and growth in the international trade, hence contributing to the achievement of the United Nations 2030 SDGs (Sustainable Development Goals). However, these gains happen at the cost, of cybersecurity risk.

REFERENCES

1. Shahrin Sadik, Mohiuddin Ahmed, Leslie F. Sikos and A. K. M. Najmul Islam(2020),Towards a Sustainable Cyber Security Ecosystem, *Computers* **2020**, *9*(3), 74; https://doi.org/10.3390/computers9030074
2. Sankalp Gurjar (2021), A look at the Approach and the Preparedness, Cyber Security.
3. Massimiliano Passalacqua (2018), Cyber Security and Sustainable Development.
4. Will Erstad (2022) ,10 Cyber Security Problems Nearly Every Organization Struggles With, Rasmussen University.

20

PRIVACY AND DATA PROTECTION IN SOCIAL MEDIA AND LIABILITIES OF INTERMEDIARIES

KEYWORDS

PRIVACY, DATA PROTECTION, FACEBOOK, WHATSAPP, TWITTER, CAMBRIDGE ANALYTICA, DONALD TRUMP

CHAPTER TWENTY

PRIVACY AND DATA PROTECTION IN SOCIAL MEDIA AND LIABILITIES OF INTERMEDIARIES

AUTHORS

PRASUN SINGH, LLM, SCHOOL OF LAW, SHARDA UNIVERSITY, GREATER NOIDA, UTTAR PRADESH, INDIA

DR. RITU GAUTAM, ASSISTANT PROFESSOR, SCHOOL OF LAW, SHARDA UNIVERSITY, GREATER NOIDA, UTTAR PRADESH, INDIA

ABSTRACT

The purpose of this research paper is to deal with the liabilities of social-media intermediaries in privacy and data protection in cyberspace. In recent times, we have seen the huge role of intermediaries in securing data or disclosing it publicly, as we saw in April 2021, 533 million Facebook user credentials were gathered using a combination of old and modern scraping techniques before being distributed to a hacker forum with a contribution request by Tom Liner, a hacker. Since there is no adequate law related to data privacy in India, it is incredibly difficult to ensure the protection of privacy rights in India.

In this research paper, the author has applied doctrinal or library-based research. All the data collected in this research will be applied from secondary data like

textbooks, legal articles, law journals, laws, statutes, international treaties, legal publications, and e-resources.

With this research, we will learn about the loopholes and lack of proper laws related to data protection and privacy in our legal system. We will discuss different data protection laws around the world and the liabilities of intermediaries in countries like the U.S., the U.K., France, and Germany. To address serious cyber threats in India, we refer to the Information Technology Act of India, which was enacted to facilitate e-commerce and hence did not prioritize privacy.

In conclusion, the need for proper data protection will be discussed, and the loophole in the current legal system related to data protection in India will be analyzed. The author will also shed some light on the roles of intermediaries for data protection and what the liabilities of intermediaries are in different countries, including India.

INTRODUCTION

Social media platforms have experienced rapid expansion in recent years, and that is why they have garnered considerable research attention. While social media platforms have always been an integral part of daily life, as more and more people are getting access to the Internet, social media platforms like Facebook, Twitter, and Instagram are taking on a more prominent role in our everyday lives. Protecting user data from unauthorized parties is a major problem, and it must be done under national and international data protection laws and standards. It should be the duty of the social media platforms to ensure that they must refrain from disclosing personal information about their users' accounts. A person's privacy is not only targeted from the outside but an 80 per cent risk of attacks are discovered to be primarily due to human errors. This is because to the fact that the users themselves are unaware of the ramifications of providing personal information. The need to establish approaches for preserving users' data, such as GPS, which is used to collect the surrounding, such as location, activity, weather, and other individuals nearby. Cameras, accelerometers, gyroscopes, microphones, and other context-aware technologies rely heavily on location awareness [1].

In recent years, social media users' concerns regarding their privacy have grown. Data breaches have shocked many users, forcing them to reconsider their social media interactions and the privacy of their details. The dramatic story of Cambridge Analytica, a consultancy firm, is a case in point. The company used the personal details of over 50 million Facebook users to impact the 2016 presidential election in the United States. This and other examples have eroded public trust, leaving many people questioning if they have lost control over their data. Social media mining is a contentious strategy that has helped digital companies like Twitter, Google, and Facebook Inc., acquire exponential user growth. These Big Tech companies are building algorithms that leverage user input to learn about their preferences and retain them as long as possible on these platforms. As simple as the amount of time spent on a screen, these inputs offer the data being mined and lead to corporations benefitting substantially from leveraging that data to capitalize on incredibly precise predictions about user behaviour. When these techniques were implemented, the expansion of platforms expanded significantly; as of 2021, most of the top platforms had more than 1 billion active users monthly [2].

SOCIAL-MEDIA PLATFORMS AND INTERMEDIARIES

The word intermediary is defined under section 2(w) of Information and Technology Act, 2000, " "intermediary", to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes". The word social-media platforms fall within the definition of Intermediaries, according to Merriam-Webster, "Social-Media platforms are forms of electronic communication (such as websites for social networking and microblogging) through which users create online communities to share information, ideas, personal messages, and other content (such as videos)". According to a 2019 Pew Research Centre survey on social networking sites use in the United States, 72 % of Americans use social media in some capacity. In 2005, the year after Facebook launched, that figure was 5%.

Social media has a far longer history than you would assume. While it may appear to be a fresh trend, websites such As Facebook are the inevitable result of decades of social media growth. Six Degrees, the first identifiable social media site, was founded in 1997. It allowed users to create a profile and connect with other individuals. In 1999, the first blogging websites gained popularity, starting a social media trend that continues to this day. Even with millions of members, users did not have a large number of direct friends, and Six Degrees lacked capabilities beyond texting. The website was ultimately shut down in 2000 [3].

Throughout and after this period, more websites began incorporating social networking platform elements into their current material, thereby transforming themselves into social media platforms, with varying degrees of success. In the years that followed, new social media platforms began from scratch and expanded beyond just listing and browsing friends. With the advent of the LiveJournal publishing site in 1999, another early type of digital social communication, weblogs, or blogs, gained prominence. This was at the same time that Pyra Labs, a software start-up that was bought by Google in 2003, launched the Blogger publishing platform. Social media gained in popularity with the development of blogging. In the early 2000s, sites like MySpace and LinkedIn gained popularity, while Photobucket and Flickr enabled online photo sharing. YouTube launched in 2005, ushering in a whole new era of communication and sharing across huge distances. Facebook and Twitter were both available to people all around the world by 2006. These sites are still among the most popular social networking sites on the web. Pinterest, Tumblr, Foursquare, and Spotify were among the first sites to emerge to serve unique social networking niches. There are a plethora of social media sites available today, and many of them may be linked to enable cross-posting. This offers an atmosphere in which users may communicate with the maximum number of people while maintaining the intimacy of one-on-one contact. We can only speculate on how social networking will evolve over the next decade or even 100 years from now, but it will certainly remain in some form for as long as people exist.

Types of Social Media Platforms:

There are virtually no categories for social media platforms in the scientific literature, though some pseudoscientific blogs or marketing resources give important perspectives on the subject. Some sources examine topical emphasis [4], while others examine topical specificity (or user base breadth) [5]. Nonetheless, some sources categorise social media platforms according to their network's openness [6], or the sort of networking that goes on. We will attempt to arrange our knowledge of what social media sites signify to their users in the following section. We'll examine the objective or functionality that a social media network aspires to provide its users. Examples of social media platforms are provided, and they are labelled according to how they market themselves; some expressly include the .com suffix. One may draw a broad contrast between social media platforms that prioritize connections and those that prioritize content.

1. **Connection based Social Media platforms:** Connection social media platforms place a greater emphasis on the relationships that users already have and make use of this by (re-) connecting users and by offering a social contact book. Social medias' main objective is to enable you to interact with people, develop communities and organisations, and exchange ideas, information, and interests. Below we will discuss various types of Connecting social media platforms: -

   Messaging sites or applications: These social networking apps have grown to be more than simply a tool to send and receive text messages. Calling, forming groups, broadcasting messages to many people, transferring money, and the ability to create chatbots are becoming part of human life. These sites or applications are also helpful for businesses we have seen that lots of hotel booking sites sends the booking confirmations on WhatsApp providing customers quick and easy customer experience.

   Dating: Dating sites are websites or applications that assist people to discover the love of their lives, and many of them now include social media features. Each user has a username and password, as well as a profile to attract future loves. Love interests are the most prevalent kind of connection, although friendship bonds and groups are also popular. Messages exchanged between users are frequently kept secret, while in certain situations, comment sections are made available to everyone. The social media platforms may retain behavioural data to provide more accurate suggestions. Examples of Dating sites or applications are Tinder, Bumble, OkCupid, Match.com etc.

   Business or Professional sites: These social media platforms aim to provide professionals with useful business contacts. Searching for profiles does not always require signing up. Profiles show a person's capabilities and field of work, as well as provide contact information for that individual. Education qualifications and alumnus status are also shown in these platforms and you can connect to people related to your qualifications or job area. Moreover, users can add other users to their network (connection) so that more professionals can see with whom the user is currently working or communicating. LinkedIn is a fine example of this class, for its premium service you need to get paid subscriptions.

   Socializing or Social networking: Representing social networks more conventionally. Here, people may stay in touch with old friends and make new ones. These platforms allow you to interact with people and companies, create or join groups, post photographs, videos, links, go live, and locate events in your immediate area. You can also purchase and sell locally through the marketplace. A well-known social networking application or website is Twitter, you can post text-based material, videos, and photos. When it comes to news, entertainment, sports, and even politics, it has become the go-to source for the newest information. Using Twitter's real-time sharing feature is its most important feature. Unlike most other platforms that do not have a character restriction of 280, this one does, however it allows you to make your message brief and to the point. For a user, the worth of such a social media network is frequently judged mainly by the number of friends they have or the number of subscribers or followers one has. Facebook, Twitter, Instagram, Orkut, and MySpace are all well-known examples of this platform.

2. **Content-based Social Media Platforms:** Content-based social media platforms are primarily concerned with the content that users offer or connect to. Following are the types of content-based social media platforms: -

   Gaming or Entertainment platforms: These platforms are mainly tied to gamers or gaming communities. Typically, the profile includes a gaming character and connection to other gamers. Messages can be sent to other users, and groups can occasionally be created. Behavioural data is generally used to keep track of the games you've played and the accomplishments you've acquired within them; this data is then shown on your profile. Entertainment social media platforms may profit from the sale of games and game add-ons, as well as subscriptions. Example of these platforms is PUBG, Call of Duty, Need for Speed, GTA, etc.

   Content Sharing: User-generated material can be shared with a small number of people, such as family or friends, or with a much larger audience. Because multimedia content is too large to e-mail to all persons involved, it is frequently shared. Users must sign up and log in to upload material; viewing content may also require signing in or knowledge of a difficult-to-guess obfuscated URL. The material suggestion may be an intrinsic element of the system, especially in more open systems, where messages or tags can be added to the shared content. If there are any, user profiles are generally brief. Examples are Picasa and Photobucket.

   Photo and Media sharing Application and Sites: On one of these platforms, a user can share photos, videos, and stories with a myriad of different filters. You can also upload 30-second vertical videos called Reels, post on IGTV for long-form video content, and even go live on sites like Instagram. A website like YouTube, despite not being a search engine, has the second-highest number of searches after Google. YouTube contains a wide range of video material, including how-to, TV episodes, songs, movies, and ads. If it's in video format, it's on YouTube. It's simple to create and share video material, and you can even go live on it.

   Content Recommendation or Discussion Forums: In certain circumstances, people choose to suggest existing (typically professional) material rather than uploading (multimedia) content. Discussion forums such as Quora and Reddit use a simple Q&A style in which helpful answers are upvoted and unhelpful answers are downvoted. A user account is represented as u/"username" on sites like Reddit, and subreddits are represented as r/"topic." Subreddits are online communities devoted to a particular topic, problem, or question. When you remark, share links, and be downvoted or upvoted, you will earn Karma Points as an active contributor in these communities. Redditors' Karma Points are similar to scorecards. Quora uses the same Q&A system like Reddit.

Users might have a variety of motivations for utilising a social media platform. Anyhow, to receive the necessary functionality (recommendations, drawing an audience, receiving advice, etc.), they will need to share some information with the social media platforms. The type of user data in question is determined by the capability of the social media platform as well as the number of media available on it.

DATA PROTECTION AND PRIVACY ISSUES

The Digital India initiative has evolved into a movement aimed at empowering ordinary Indians via the use of technology. The widespread use of mobile phones, the Internet, and other technologies has also facilitated the expansion of several social media platforms in India. The main objective of the Social Media Platform is to share content with as many people as possible. Users post their normal activities on social media platforms such as Facebook, Twitter, and LinkedIn. Social media platforms users occasionally share information about themselves and their life with their friends and colleagues. However, some of the shared data via social media platforms are private and should not be shared on public platforms. Typically, users share portions of their everyday lives via status updates or through the posting of images and videos. Currently, a variety of social media platforms users use smartphones to capture images and create films for sharing over these platforms. These data may include location information and other metadata.

Ascertaining social media platforms can execute desired behaviour is one thing; nevertheless, while sharing a wealth of (personal) data, one should also consider the possibility of undesirable conduct. Social Media services collect a variety of data about their customers to deliver individualised services, but this data may also be used for commercial purposes. Additionally, users' data may be shared with third parties, resulting in privacy breaches. The word "privacy" has a variety of somewhat diverse definitions, ranging from personal privacy (which encompasses isolation and physical privacy) to information privacy. Privacy on the Web in general is primarily concerned with Information Privacy, as described below in the IITF wording used by Kang [7].

"Information Privacy is "an individual's claim to control the terms under which personal information–information identifiable to the individual–is acquired, disclosed or used."

In a Web2.0 atmosphere, where users interact and exchange information, the protection of personal privacy of information becomes critical. This information can be used by malicious people to exploit and compromise an individual's privacy. Information retrieval and data privacy are two rapidly emerging fields of computer science with distinct objectives. Methods for data extraction are provided by information retrieval. Additionally, it provides an organization with a set of methodologies for data analysis and decision-making based on the obtained information. Privacy entails limiting the scope of information. This scope is defined by the audience's size (breadth), the amount of permissible usage (depth), and the length (lifetime). When data is sent outside of its intended scope (accidentally or deliberately), privacy is compromised. A breach occurs whenever data is shared with a party that was not intended to receive it (disclosure). Additionally, it can occur when information is exploited for a purpose other than that for which it was intended, or when information is accessed after its intended lifespan has expired. This is also reflected in data protection legislation, such as the United Kingdom's Data Protection Act 1998 [8], which imposes constraints on the scope and duration of personal data usage. With the rise of social media and the increasing popularity of online communication via social media platforms, individuals' sensitive information is becoming increasingly accessible online. While the majority of the material provided on social media platforms is not sensitive, some individuals disclose personal information. Thus, the availability of sensitive data to the public might result in the exposure of user privacy. Users' privacy is compromised when publicly available data may be traced and their behaviours can be linked to this data for mining and extracting sensitive information.

Palen and Dourish [9] differentiate three types of privacy boundaries with which humans struggle: -

1) The disclosure boundary (managing the tension between private and public),
2) The identity boundary (controlling one's self-image about a certain audience, e.g., one acts differently at work than with friends),
3) The temporal boundary (managing past actions with future expectations; user behaviour may change over time)

Weiss [10] compares the old view of privacy with the increased demands for privacy created by social media platforms. Users' identities are hidden and only authorized parties are granted access to their data on the conventional Web to protect their privacy. When it comes to social media platforms, the fact is that data and identity are inextricably intertwined, and both are frequently exposed to large groups of people. This makes privacy and information management much more difficult, and it gives rise to privacy concerns. The majority of social media platforms have privacy options that are simple to use, yet insufficient. They frequently demand the user to select whether each profile item should be visible to friends only, friends and family, or the whole public. Occasionally, a few more selections are shown. It all comes down to a list of items with checkboxes to indicate whether or not the contents should be disclosed to specific groups, hence restricting the amount of control the user has.

Most Internet users want to know that any personal information they provide will not be shared with anybody else without their consent. The link between the collecting and distribution of data, technology, the public expectation of privacy, and the legal and political concerns surrounding them is known as information privacy (or data protection). Whenever personal information or any other sensitive data is gathered and kept – whether digitally or otherwise – privacy problems arise. Inadequate or non-existent disclosure controls might be the source of privacy concerns. Users face a new set of privacy problems as the amount of personal information they disclose online increases. Personal material is becoming increasingly easier to post thanks to digital cameras and, more recently, a new class of camera phone applications that can upload photographs or video content directly to the web. Privacy problems are particularly severe in the case of multimedia collections, as they have the potential to expose a great deal about a user's personal and social life.

User-related Privacy Issues Vs. Provider-related Privacy Issues: We may divide privacy threats into two categories: those involving disclosure to other "users" (registered or not), and those originating from the social media platform's service provider**.** The sort of information that each of these parties has access to is the primary distinction between them. In most cases, a user or an outsider can only examine publicly available information. The social media provider often has access to all of the data stored on the system, including private uploads, browsing activity, IP addresses, and other information. When it comes to the connection between a user and a service provider, trust is extremely important. The fact that both categories of threats require their particular protection measures is because the types of access differ substantially. Awareness of the need to safeguard user data from other users, as well as appropriate tools for administering and enforcing access controls, are critical components of data protection [11, 12]. This is ineffective in resolving concerns involving untrustworthy service providers. The common strategy is to obscure and hide sensitive data from providers [13,14] or to completely remove them from the picture [15,16].

User-related Privacy Issues: In many circumstances, OSN users or unregistered visitors breach privacy. Snooping and hacking, as well as inadvertent mishandling of privacy settings by the user, can lead to catastrophic repercussions. This can be purposeful or accidental. Here are some examples of dangers to your privacy that entail disclosing personal information to other people.

1. **Confidential Details:** Users may mistakenly believe that some information will be kept confidential when, in fact, it will not be. This might be as a result of design faults on the side of the social media service provider (for example videos, photos, and blogs being hacked on MySpace [17]), or a failure to comprehend or pay attention to privacy measures by the user himself. It might also be caused by data retention issues, in which case a resource may be removed or deactivated, but references to it (thumbnails, messages on friends' profiles, and so on) are still available to the outside world due to data retention issues. When a stranger has access to such sensitive information, it is considered a violation of the disclosure boundary. The user no longer has control over who receives his or her personal information. In this case, the problem is associated with your profile, your relationships with other members of the site's user community, communications, multi-media, tags, or group membership. Rosenblum [18] demonstrates that data on OSNs is significantly more accessible to a broader audience than its owners believe, and that information on OSNs can even wind up in the mainstream media [19]. Even the most experienced internet security professionals might make blunders when it comes to sharing information [20].

2. **Unable to Hide Information from a particular group or friend:** There are instances when you'd wish to keep some information from a specific friend or a group of friends. Perhaps you do not want to tell a friend that you are arranging a surprise party for his birthday, or you do not want your parents to see the images of your night out. In real life, we can simply control the many social situations to which we belong, but in social media platforms, the boundaries between them tend to disappear [21].

3. **Other User Posting your Data or Information:** While you can control what information you want to post on your social media platform, you have no control over what other users post on their social media platforms about you. Because information is made more widely available than was intended, there is an issue with the disclosure boundary. In some cases, it might happen when a person uploads information about you that you don't want to appear on the social media platform, or when a user discloses private information about you to another user. Sometimes act like this are done purposefully [22].

Provider-related Privacy Issues: In contrast, a completely separate form of privacy threat concerns the relationship that exists between a user and a social media service provider, and more specifically, the level of trust that the user places in the provider**.** This extends beyond the control of information by the user because the provider is often responsible for designing or configuring the technologies that underpin the social media platforms. Subsequently, the service provider has access to any user-related data, such as browsing history and message records. Below are the details of some of the related threats.

1. **Data Retention:** When you upload information to a social media platform, it is mostly impossible or extremely difficult to take that material off again. In the case of Facebook, for example, users cannot remove their profile, and the company has actively prevented third-party software that seeks to solve this situation [23]. Even data that appears to have been removed from the social media platform can be found elsewhere on the network, for example in backups or on their servers. Because the information is available for a longer period than intended, this is a violation of the temporal boundary. Bonneau [24] illustrated this when he monitored the availability of removed images on the internet. Additionally, Facebook would prefer to save content for an indefinite period [25].

2. **Social Media Platforms Employee Browsing Personal Data:** Social Media Service provider has complete access to the data, which an employee of the service provider might misuse. This runs counter to the implicit trust needed by social media platforms. All information given to social media service providers is at risk in this situation, including behavioural information, which is not uncommon. According to interviews, certain Facebook workers have access to user information, and it is up to the company to ensure that this does not happen [26].

3. **Targeted Marketing:** Multiple pieces of information on social media platforms can be merged to create high-value user data based on the information available. It is possible to use or exploit this high-value profile to provide tailored marketing to the consumer. This is another instance of a conflict with the implicit trust that the social media platform has when information is utilized in a manner that is different from that intended by the user [27]. TrustFuse is an example of a corporation that makes use of social media data for targeted marketing purposes.

   "According to TrustFuse's Web site, all of this information might be useful for Rapleaf's third business, TrustFuse, which sells data (but not e-mail addresses) to marketers so they can better target clients."

4. **Selling of user Data and Information:** The vast amount of data stored on social media platforms is likely to be valuable to external parties, and social media platforms may sell it. User behaviour, pref-

erences, and friendship connections can all be useful for marketing and social dynamics study. Data sales can easily collide with the user's implicit trust on social media platforms. PatientsLikeMe is a fine example of an intermediary that shares user data with other parties.

"Pharmaceutical corporations get access to thousands of chronic illness sufferers through PatientsLikeMe.com. Keep an eye on their symptoms and treatment outcomes, as well as their attitude. Use real-world safety and effectiveness data to perform focused clinical trials. A few instances of how our services contribute value throughout the drug development process are included in this list."

DATA MINING BY SOCIAL MEDIA PLATFORMS

Social media mining is the process of extracting large amounts of data from user-generated content on social media websites and mobile apps to identify patterns, draw conclusions about users, and act on the data, most frequently for advertising to users or performing research. Data mining is also referred to as database mining, information harvesting, knowledge mining, knowledge extraction, data dredging, data pattern processing, and data archaeology. Data mining is the act of examining data from a variety of different dimensions or perspectives and condensing it into valuable information that can be employed in a variety of industries to aid in decision-making. Data mining is a technical term that refers to the process of detecting patterns or correlations in big relational databases using methods from artificial intelligence, machine learning, statistics, and database systems.

The use of social media websites has increased dramatically in recent years. This tendency is not limited to personal websites, but also corporate websites. These later platforms host a massive quantity of data that has been uploaded by consumers or users. As expected, the data on business social media websites is typically linked to the firms' products or services. As a result, the data may be used to benefit businesses. For instance, operations management studies and practices to make the process and product design decisions [28]. As data mining's value continues to rise, it has been applied in a variety of areas, including sales/marketing, insurance, banking, finance, telecommunications, medicine, fraud detection, and the education sector [29][30][31][32][33].

A hacker going by the name of Tom Liner catalogued information compiling a database of 700 million LinkedIn members from around the world and selling it for roughly $5,000 (£3,600; €4,200). The event, along with other comparable incidents of social media scraping, has ignited a contentious discussion about whether or not the basic personal information we provide openly on our profiles should be properly safeguarded [34]. Social Media mining is a contentious activity that has enabled internet companies such as Google, Twitter, and Facebook Inc., to increase their user bases. These corporations, termed as "Big Tech," develop algorithms that use user input to learn their preferences and keep them on their platforms as much as possible. These inputs, which may be as simple as time spent on a particular screen, offer the data for mining, and firms gain financially from their use of that data to make incredibly precise predictions about user behaviour. Platforms grew significantly after these techniques were implemented; the majority of the leading platforms currently have an average of more than 1 billion monthly active users by 2021 [35].

CHALLENGES FOR INTERMEDIARIES AND SOCIAL MEDIA PLATFORMS AND THEIR GOVERNANCE

These social media platforms have enabled ordinary Indians to express their creativity, ask questions, stay informed, and openly share their opinions, including criticism of the government and its officials. The Government recognises and respects each Indian's freedom to criticise and dissent as a necessary component of democracy. India is the world's largest open Internet society, and the government encourages social media businesses to establish operations, do business, and generate profits in India. They will, however, be held accountable to India's Constitution and laws. Recently, several extremely concerning trends have been noted on social media sites. Due to the persistent circulation of fake news, several media outlets have included fact-checking tools. The widespread use of social media to post morphed photographs of women and content connected to revenge porn has frequently jeopardized women's dignity. The unethical use of social media to settle corporate conflicts has become a major source of worry for corporations. Through platforms, instances of harsh language, libellous and obscene information, and flagrant contempt for religious sensitivities are increasing. Over the years, the rising occurrences of criminals and anti-national groups misusing social media have created new obstacles for law enforcement agencies. These include inducing terrorist recruiting, publishing obscene information, causing division, perpetrating financial fraud, inciting riots, and disrupting public order. The most significant obstacle provided by social media is the issue of privacy. Many people are reluctant to participate in dialogue because they are concerned about their privacy being compromised. Advertising on social media should comply with censorship guidelines, and pornographic content in ads should be avoided on websites dedicated to social media. If such limits are not strictly enforced, it is possible that youth's minds may be ruined, resulting in an increase in crime. In today's cyber environment, social media offers one of the most significant issues. The identification of the person who joins social media websites may be genuine or fake. The other user is unaware of the genuineness of his/her identification. Many examples of deception have been reported in recent times all across the world. Social media has shown to be a simple means of deceiving people through the use of technology.

The Information and Technology Act (IT ACT): The word intermediary is defined under section 2(w) of Information and Technology Act, 2000, " "intermediary", to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes". Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (the "Intermediary Rules") governs intermediaries in India. It is believed that the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (the "Intermediary Rules") would significantly change how Indians interact with the internet.

While Part I of the Intermediary Rules is primarily concerned with the definitions, Parts II and III of the Intermediary Rules are concerned with the actual compliances and obligations. Part II of the Act deals with the regulation of intermediaries, which includes social media intermediaries, Messaging-related intermediaries include apps like WhatsApp, Twitter, and Signal while media-related intermediaries include sites like Snapchat, Facebook, Twitter and Instagram. The Ministry of Electronics and Information Technology, also known as MeitY, is in charge of administering this area. Part III deals with the regulation of digital news media (though it is unclear which news organizations are covered by such Rules), as well as over-the-top (OTT) services such as Disney+Hotstar, Netflix, and Amazon Prime. The Ministry of Information and Broadcasting is in charge of administering Part III. Under the rules, all social media platforms are required to establish a grievance redressal and compliance system, which included the appointment of a resident grievance officer, a chief compliance officer, and a nodal contact person. The Ministry of Electronics and Information Technology (MeitY) had also requested that these platforms give monthly reports on complaints received from users and the actions taken in response to such complaints. The third requirement was for instant messaging apps to include the features that allowed users to track down the person who is the originator of a message. This raises the necessity of traceability, which would render end-to-end encryption ineffective. If any of these standards are not met, the indemnity offered to social media intermediaries under Section 79 of the Information Technology Act would be revoked.

LAWS TO REGULATE INTERMEDIARIES IN DIFFERENT COUNTRIES AROUND THE WORLD

When it comes to our daily Internet use, intermediates play a crucial role: accessing the Internet, browsing it, engaging in e-commerce, and creating content are all made possible by the efforts of intermediaries. Even though they are commonly referred to as Internet Service Providers (ISPs), online intermediates are a diverse group of services that include search engines, hosting services providers, e-commerce platforms, social networking platforms, etc. Intermediary liability is a legal concept that refers to an intermediary's responsibility for the material it stores and transmits. This type of information might include hate speech, breach of copyright, pornographic content or photographs of abuse.

In the United States, Section 230 of the Communications Decency Act, 1996 protects internet services, including intermediaries, from responsibility for the transmission of any third-party content. It specifies expressly that suppliers of 'interactive computer services are not considered publishers of third-party content. Additionally, the clause specifies that such internet services may review and remove offensive or obscene third-party content in 'good faith.' This has resulted in the development of platform-specific 'community guidelines' and regulations about the acceptability of material for each such site. This is a significant departure from India's position on intermediary regulation, as the IT Act makes no provision for content filtering methods. In Feb 2020, the United States Department of Justice hosted a day-long meeting to consider potential amendments to Section 230. They're looking at instances in which networks permitted the circulation of non-consensual pornography, harassment, and pictures of child sexual abuse. The Digital Millennium Copyright Act (DMCA) was passed in the United States in 1998. According to the DMCA's Section 512, Intermediaries are exempt from paying damages for infringements of copyright that occur on their networks if certain requirements are met. If the intermediaries don't comply with this notice and takedown procedure, they will be held responsible for any infringement claims made by copyright owners [36].

In October 2017, Germany passed the Netzwerkdurchsetzungsgesetz (NetzDG) or the Network Enforcement Act, which forces digital firms to remove "obviously illegal content" within 24hrs of being notified. Other unlawful content must be examined and removed within a week of being notified. Despite the criteria being based on vague and confusing phrases like 'insult' or 'defamation,' non-compliance can result in fines of up to €50 million (EUR). The Bundestag enacted NetzDG legislation in 2020, requiring social media platforms to report some sorts of illegal content to Germany's Federal Criminal Police Office. Since the new German law was enacted, at least 13 nations, including the European Commission, have implemented or proposed intermediary liability schemes that are generally comparable to the act's matrix.

The Draft Online Safety Bill was introduced into the United Kingdom Parliament in May 2021. Users-generated material must be monitored by internet service providers to protect customers from being exposed to unlawful or harmful content on the internet, according to proposed legislation. Among the most significant additions is the idea that tech firms should designate a "safety controller," who would be held responsible for an offence if there were "repeated and systematic failures."

French lawmakers passed new legislation in May 2020 that forces social media sites to delete specific offensive and illegal content within 24 hours of receiving it. By the law, big operators of online platforms whose business involves connecting multiple people to share content are required to remove content that condones certain crimes or causes discrimination, hatred, or violent behaviour, violations of human rights, aggravated personal attacks, harassment, or paedophilia within 24 hours of receiving user notifications.

CONCLUSION

Users might have a variety of motivations for using social media services. If they want to use the required functionality (recommendations, attracting an audience, receiving advice, and so on), they will need to disclose some information about themselves to the social media platforms. The kind of user data in question is determined by the functionality of social media platforms as well as the amount of material available on those platforms. Because of the trade-off between functionality and privacy, the possible sensitivity of data, and the open nature of internet systems, privacy is unquestionably a concern for many people. Because social media platforms or intermediaries include vast amounts of usable and interesting data from large numbers of users, they are a desirable target for third parties, whether private or commercial, due to the large amounts of useful and interesting data they have. This information might land up in the wrong hands through a variety of means, including browsing/spidering, cyber-attacks, or basic data trades. Users and social media platforms can have competing interests because users are not necessarily the source of money for social media platforms (as in the case of advertisement revenue and data sales). Because of the broad and frequently comprehensive information available on social media platforms, as well as the fact that threats might come from other users or even the provider itself, the risks are multiple and diverse. If we enforce a set of well-defined policies for social media, such as a strong password, awareness of changing passwords frequently, the purpose of antivirus or related software, awareness of information disclosure, and proprietary software, we can protect the social media platforms or intermediaries from further attacks and vulnerabilities. The alarming potential for these platforms to gather information on its users indefinitely without their explicit agreement or knowledge, combined with the users' ignorance and uncaring attitude toward this, is what privacy activists are most worried about. Thus, the existing quo requires and necessitates that people's data be safeguarded by the courts, if not the government.

REFERENCES

1. Pramod Jagtap, Anupam Joshi, Tim Finin, and Laura Zavala, "Preserving Privacy in Context-Aware Systems," Fifth IEEE International Conference on Semantic Computing, 2011, pp.149-153.
2. McCourt, Abby. "Social Media Mining: The Effects of Big Data in the Age of Social Media". Media Freedom & Information Access Clinic. Yale Law School. Retrieved 25 February 2021.
3. [3] D. Boyd and N. B. Ellison. Social network sites: Definition, history, and scholarship. Journal of Computer-Mediated Communication, 13(1):210–230, 2007.
4. Gautam, R., Kulshrestha, P., & Goswami, M. A. K. (2021). Mediation And Family Dispute Resolution Mechanism: A Case Study On Clinical Legal Education. Elementary Education Online, 20(3), 2490-2490.
5. Gautam, R., "Proliferation of Cyber Crime and Indian legal system with special reference to Gwalior Division" Available at: https://shodhganga.inflibnet.ac.in/handle/10603/250817 Retrieved on: 22/07/2021
6. Pandey, N., Gautam, R., "property right of women in patriarchal indian society: a comprehensive study on legal narrative" Available at: https://www.researchgate.net/publication/361733554_PROPERTY_RIGHT_OF_WOMEN_IN_PATRIARCHAL_INDIAN_SOCIETY_A_COMPREHENSIVE_STUDY_ON_LEGAL_NARRATIVE_PROPERTY_RIGHT_OF_WOMEN_IN_PATRIARCHAL_INDIAN_SOCIETY_A_COMPREHENSIVE_STUDY_ON_LEGAL_NARRATIVE
7. Gautam, R., Medical health condition of prisoners and discrepancy in facilities among the states of Uttar Pradesh, Haryana and Delhi, International Journal of Health Sciences Follow journal, DOI: 10.53730/ijhs.v6nS6.12256
8. R. Dube and M. B. P. Adomaitis. What types of social networks exist? online, 3 2009. http://socialnetworking.lovetoknow.com/What_Types_of_Social_Networks_Exist.
9. E. Burns. Marketing to social networking sites, targeted. online, 4 2007. http://www. clickz.com/3625536.
10. B. Lunn. Social network types, motivations, and the future. online, 9 2007. http://www. readwriteweb.com/archives/social_network_types_motivations.php.
11. J. Kang. Information privacy in cyberspace transactions. Stanford Law Review, 50(4):1193– 1294, 1998

12. S. Buchegger, D. Schioberg, L. H. Vu, and A. Datta. Peerson: P2p social networking: early ¨ experiences and insights. In SNS '09: Proceedings of the Second ACM EuroSys Workshop on Social Network Systems, pages 46–52, New York, NY, USA, 2009. ACM.
13. A. Jacob. How to hack myspace private profile picture and video. online, 4 2007. HTTP:// www.clazh.com/how-to-hack-myspace-private-profile-picture-and-video/.
14. D. Rosenblum. What anyone can know: The privacy risks of social networking sites. IEEE Security & Privacy, 5(3):40–49, May 2007.
15. N. Hernandez. President apologizes for questionable photos, 10 2007. http://www. washingtonpost.com/wp-dyn/content/article/2007/10/17/AR2007101702244. HTML.
16. D. M. Williams. Online identity expert loses control of nsfw r-rated online pics, 3 2009. http://www.itwire.com/your-it-news/home-it/ 23975-online-identity-expert-loses-control-of-nsfw-r-rated-online-pics.
17. Gautam, R., Kanpur Philosophers ISSN 2348-8301 Vol IX, Issue V (IV), 2022151EFFICACY OF PROCEEDINGS OF CONCILIATION AND SETTLEMENT OF ANINDUSTRIAL DISPUTE UNDER INDUSTRIAL DISPUTES ACT, 1947, A CRITICAL Analysis. Available from: https://www.researchgate.net/publication/361733673_Kanpur_Philosophers_ISSN [accessed Sep 11 2022].
18. Gautam, Ritu, Cybercrimes and International legal regime, Available at: https://shodhganga.inflibnet.ac.in/bitstream/10603/250817/10/10_chapter-iv%20%20cybercrime%20issues%20and%20international%20legal%20regime.pdf
19. Gautam, Ritu, Cyber crime in India, Availablr at: http://hdl.handle.net/10603/250817
20. R. Lee. Context Is Everything - Sociality and Privacy in Online Social Network Sites, volume 320/2010, chapter 4, pages 48–65. Springer Boston, 2010.
21. [W. Riddle. Cyberbullied teen sues ex-classmates, their parents, and Facebook 3 2009. http://www.switched.com/2009/03/04/ cyberbullied-teen-sues-ex-classmates-their-parents-and-facebook/.
22. P. MacNamara. Facebook blocks 'web 2.0 suicide machine'. online, 1 2010. http://www.networkworld.com/news/2010/ 010410-buzzblog-facebook-blocks-suicide-machine.html.
23. J. Bonneau. Attack of the zombie photos. online, 2009.
24. http://www. lightbluetouchpaper.org/2009/05/20/attack-of-the-zombie-photos/.
25. C. Walters. Facebook's new terms of service: "we can do anything we want with your content. forever.", 2 2009. http://consumerist.com/2009/02/ facebooks-new-terms-of-service-we-can-do-anything-we-want-with-your-content-forever. Html
26. N. O'Neill. "anonymous" Facebook employee interview: Fact vs fiction, 1 2010. http://www.allfacebook.com/2010/01/ anonymous-facebook-employee-interview-fact-vs-fiction/.
27. S. Olsen. At Rapleaf, your personals are public. online, 8 2007. http://news.cnet.com/ At-Rapleaf,-your-personals-are-public/2100-1038_3-6205716.html.
28. H. K. Chan, E. Lacka, R. W. Y. Yee and M. K. Lim, "A case study on mining social media data," 2014 IEEE International Conference on Industrial Engineering and Engineering Management, 2014, pp. 593-596, doi: 10.1109/IEEM.2014.7058707.
29. Neelamadhab Padhy1, Dr Pragnyaban Mishra 2, and Rasmita Panigrahi3, "The Survey of Data Mining

Applications And feature scope", in International Journal of Computer Science, Engineering and Information Technology (IJCSEIT), Vol.2, Issue.3, 2012

30. Smita1, Priti Sharma, "Use of Data Mining in Various Field: A Survey Paper", in IOSR Journal of Computer Engineering (IOSRJCE), Volume 16, Issue 3, PP 18-21, 2014.
31. Mrs Bharati M. Ramageri," DATA MINING TECHNIQUES AND APPLICATIONS", in Indian Journal of Computer Science and Engineering, Vol. 1 Issue. 4, PP: 301-305
32. Annan Naidu Paidi "Data Mining: Future Trends and Applications" in International Journal of Modern Engineering Research (IJMER), Vol.2, Issue.6, PP:4657-4663, 2012.
33. Umamaheswari. K, S. Niraimathi "A Study on Student Data Analysis Using Data Mining Techniques", in International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 8, PP:117-120, 2013.
34. Tidy, Joe. "How Your Personal Data Is Being Scraped from Social Media." BBC. July 16, 2021. https://www.bbc.com/news/business-57841239.
35. McCourt*, Abby*. "Social Media Mining: The Effects of Big Data in the Age of Social Media". *Media Freedom & Information Access Clinic. Yale Law School.* Retrieved 25 February 2021.
36. Joy, Steena. "Digital Media Ethics And Intermediary Liability: How Other Countries Have Approached It." May 28, 2021. https://ca.movies.yahoo.com/digital-media-ethics-and-intermediary-liability-how-other-countries-have-approached-it-113901599.html.

21

CYBER CRIME: LEGAL ISSUES AND ITS LEGAL REMEDIES

KEYWORDS

CYBER-CRIME, HACKING, CYBERSECURITY, SYSTEM-INTRUSION, DATA THEFT, IDENTITY THEFT, PHISHING, CYBERSPACE

CHAPTER TWENTY ONE

CYBER CRIME: LEGAL ISSUES AND ITS LEGAL REMEDIES

AUTHORS

SADAF WASEEM, PH.D. SCHOLAR, SHARDA SCHOOL OF LAW, SHARDA UNIVERSITY, GREATER NOIDA, UTTAR PRADESH, INDIA

DR. ROHIN KOUL, SHARDA SCHOOL OF LAW, SHARDA UNIVERSITY, GREATER NOIDA, UTTAR PRADESH, INDIA

ABSTRACT

Cybercrime, e-crime, Internet scams, etc. are all terms used to describe illicit activities using one system or a whole network. With the development of technology and also the Internet's secretive character, it is now possible for people with little technical ability to generate money fraudulently without leaving their house, and cybercrime is rising as a vocation. These dangers are growing every day; in fact, recently some of the largest attacks ever were recorded and predictions indicate that things will only get worse from here on out. The need for cyber laws and worries of the government authorities are brought on by the rising number of crimes. This paper provides overview of several countries' cyber laws, highlighting the problems and potential legal repercussions. Here, it is examined whether and to what extent these laws are sufficient to safeguard us. These rules cannot keep up with the fast-evolving cybercrime scenario.

> *True Cybersecurity is preparing for what's "Next", not what was "Last".*
> *-Neil Rerup*

INTRODUCTION

A general definition of cyber law states that it is a legal framework that governs all legal issues relating to the internet, cyberspace, computer systems and information technology. A vast spectrum of subjects is covered under cyberspace law, including contract law, privacy legislation, and intellectual property laws. It oversees electronic commerce as well as the distribution of software, data security and information. Cyber law gives e-documents legal validity. The system also offers a framework for filing forms electronically and conducting e- commerce transactions. Simply described, it is a statute that addresses cybercrimes. As electronic-commerce has grown in popularity, it is now crucial to make sure that the right policies are in place to stop fraud.

Cybersecurity is governed by a wide variety of laws, many of which are spatially territorial in nature. The penalties for the same, range from fines to prison depending on the offense committed. The first Cyber law to ever be passed was the Computer Fraud and Abuse Act of 1986. It forbids the misuse of digital data as well as unlawful computer access.

Cybercrimes have increased along with internet usage. Today's media is filled with reports of various cybercrimes, including child pornography, crypto-jacking, identity theft, cyberterrorism and many more. In cybercrimes, a computer is either a tool, a target, or both that is used to carry out illegal activity. Electronic commerce and online stock trading have dramatically increased in our quickly evolving digital age, increasing the number of cyber-crimes.

There seem to be three ways that computers can be used in criminal conduct: as a tool of crime, as victim of the crime, and as an inadvertent part of the crime. The distinctive element is how a computer is specifically utilized from the perspective of the criminal.

Cybercrime has a long history and isn't a recent phenomenon, much like crime does not constitute a new concept.

The use of computers in criminal activity is something new. Nowadays, organized crime, like controlled botnets as well as activities intended to harm specific targets, has taken the role of ordinary teenage hacking.

Law enforcement has faced difficulties in responding towards the increased threats produced by rampant crime, and the judicial process has been reluctant to move. Most people picture a computer being targeted and assaulted by an intruder when they think of cybercrime. The offender tries to profit from some kind of computer-related illegal conduct.

Cybercrime in the 1980s and 1990s was primarily comprised of viruses and worm-attacks, each of which caused some kind of harm but yielded little profit for the perpetrator. With the development of new viruses, targeted attacks, rootkits, and advanced threats in the twenty-first century, criminals could now target specific users and respective bank accounts.

In the present environment, it is simple to forecast where this type of attack will take place—where there's money, there's a criminal motive.

Computer-based scam, such as click-fraud and IT call-centre fraudsters, is a frequent type of criminal conduct.

Fraudsters frequently target Amazon and eBay. Whether a fraud is performed through a false listing, a false bid, or blatant theft of goods, the outcome is the same: a crime is committed. Internet banking and trading platforms are becoming more popular with users, and vice versa. On Internet, it's typical to find malware that installs a keyboard logger and then keeps an eye out for logins to banks and brokerages.

The attacker might start robbing accounts as soon as they identify their targets.

They have a very minimal chance of being discovered and facing charges. The likelihood that you will serve federal prison time when the FBI tracks you down and puts handcuffs on your wrists, is better than 95% if you rob a bank in United States. However, the chances of the reverse happening are much better if you conduct it online: less than 1% of such offenders are apprehended and charged.

Major reason cyber-criminals are turning towards digital crime is the minimal danger of being detected. Cybercriminals of today utilize computers as instruments to steal valuable data or intellectual property, which they then resell through unofficial internet forums. The prosecution and investigation of all these crimes have become considerably more difficult for authorities as a result of the use of computers to physically separate the offender from the immediate incident of the crime.

Incidental involvement is last way that computers are used in illegal activity. Al Capone, a prominent criminal, was found guilty of tax evasion in 1931 using accounting information and tax regulations.

Computers are often used for other illegal activities, including the trafficking of child pornography. The utilization of computers is basically incidental to an offense itself because these actions were commonplace prior to the invention of computers.

Computer crime in the twenty-first century is a very complex issue given the three different ways that computers are used in criminal activities, the countless ways that criminals can steal from or defraud people, the oblique connection made possible by computers, Internet and other factors.

The FBI and National White Collar Crime Centre (NW3C) have teamed up to create Internet Crime Complaint Centre (IC3), the online clearinghouse that disseminates information on cybercrime-related issues.

A list of frequent Internet Crime Schemes, explanations of each, and suggestions on how individuals might prevent such crimes are some of the resources made available to online community.

Different Forms of Cyber-crimes

The following are seen as examples of several sorts of cybercrimes:

- Child sexual abuse material (CSAM) or child pornography:

Child sexually abusive materials (CSAMs) are, in the broadest sense, any type of media that includes sexual imagery of any kind that may show the victimized or exploited child. A clause in Section 67(B) of Information

Technology Act specifies that it is unlawful to publish or transmit any content electronically that shows youngsters engaging into sexually explicit behaviour.

- Cyber-grooming:

This phenomenon involves someone becoming close to an adolescent and then using coercion, taunting, or other methods to get them to engage in sexual activity.

- Cyber-Stalking:

Cyber-stalking is the practice of harassing or stalking a person over the internet or through other technological means. Text messages, social media posts, emails and other types of cyberstalking are frequently persistent, systematic, and planned.

- Cyber-bullying:

Someone who abuses or harasses others online, on computers, laptops, mobile phones etc., is known as a cyberbully. Bullying that takes place online is referred to as cyberbullying. Social media, chat services, mobile devices and gaming platform might all be used. This frequently entails a pattern of behaviour meant to alarm, enrage, or humiliate the target.

- Online sextortion:

When a cybercriminal threatens someone with publishing private and sensitive information online, this is known as online sextortion. These criminals use threats to coerce victims into providing them with a sexual image, a sexual favour, or money

- Online job fraud:

An online job scam or fraud strategy involves deceiving job seekers by making better, higher-paying jobs sound appealing while actually only providing them false expectations. The Reserve Bank of India (RBI) issued a warning on March 21, 2022, urging citizens not to be duped by job scams. By doing this, RBI has described how online job-fraud is carried out and the safety measures the average person should take while enrolling for whichever job, whether it be in India or elsewhere.

- Phishing:

Phishing fraud occurs whenever an email purports to come from a reliable source but actually contains a harmful attachment which is intended to steal the user's personal information, like as their ID, Card number, IPIN, CVV expiration date, etc., before selling the data on dark web.

- Credit or debit card fraud:

These crimes involve making unlawful transactions using or withdrawals from the other person's card in order to obtain their funds. Credit or debit card fraud is the use of the customer's account to make fraudulent purchases or cash withdrawals. When a criminal has access to cardholder's debit or credit number or Personal

Identification Number, fraudulent conduct takes place (PIN). Hackers or dishonest employees may get your information.

Prevention of Cyber-crime

The International Maritime Organization (IMO) has advised that the following methodology be used to approach the risk of cyberattacks:

- To specify the duties and functions of the employees in charge of managing cyber risk.
- To find the systems, resources, information, or capabilities that, if compromised, would jeopardize the operation.
- It's crucial to put risk-control procedures and backup plans in place to safeguard contra to potential cyber incident and ensure operational continuity.
- It is crucial to create and put into practice strategies for swiftly identifying cyberattacks.
- the creation and execution of plans to provide resilience and restore vital systems for ongoing operation.
- Finally, decide on and put into action the steps that need to be followed to restore and backup any impacted systems.

The following are some tactics that can be utilized to stop cybercrime:

Evaluate the risk exposure

Users must evaluate the risk and take all necessary precautions in order to be sufficiently prepared for cyber assault. Businesses ought to think about the following:

- They should take into account all potential targets for cyber-attacks and any ensuing operational weaknesses.
- To identify the systems that are most important to the operation, to comprehend the vulnerabilities that each system may have, and to gauge the effect of a cyberattack on business operations, it is required to conduct a vulnerability analysis of all the systems.
- Businesses should audit their operational technology and information technology systems.

Preventive Measures:

Adoption of International or National Technical Standards which offer a heightened level of security is advised for businesses. Companies without the appropriate financial or technical resources are advised to take these general preventative steps. The listing of preventive measures is as follows:

(i) Implementing several levels of defence, starting with physical safety, moving on through management rules and procedures, firewall, network design, computer policies, account managed services, security updates, and lastly antivirus software.

(ii) Putting into practice the idea of least privileges, which limits access and information only to the groups of people who truly require it.

(iii) Putting in place network-hardening mechanisms, making sure patch management is adequate and regularly assessed.

(iv) Using technology like Protocol-aware Filtering as well as segregation to secure important systems.

(v) Ensuring USBs connected in conjunction with another device are virus-checked and that detachable devices are secured.

(vi) Furthermore, it's critical to create business continuity strategies, identify key individuals, and put processes in place in order to stop the negative effects of a cyber-attack from worsening and restore corporate operations.

(vii) Organizing regular awareness-raising and training programs for all staff members might also be helpful.

CYBER CRIME LAWS IN INDIA

There are five primary categories of laws that need to be abided by in cybersecurity. Cyber laws have become more significant in nations like India that have extraordinarily high internet usage rates. The usage of information, e-commerce, software, and financial activities in digital world are all subject to stringent legal restrictions. Cyber laws of India have aided in the growth of e-commerce and government by ensuring maximum connection and reducing security concerns. Additionally, this has increased the scope and efficiency of digital media and made it approachable in a larger number of ways. The incorporation of cyber laws aims to establish some rules and guidelines to regulate online transactions and classify them either legal or unlawful and penalized. All forms of electronic-information are validated by the IT legislation of 2000 and cannot outpace its legal impact.

INFORMATION TECHNOLOGY ACT 2000

Overview of Act

It is the very first cyberlaw that the Indian Parliament has adopted. The following is listed as the act's object:

"To provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as electronic methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Banker's Book Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto."[1]

However, a number of legislative changes are being implemented as a result of the danger posed by cyber-attacks and people's propensity for misusing technology. It draws attention to the severe punishments and sanctions which the Indian Parliament has passed in order to defend the e-government, e- commerce and e-banking industries. It is significant to highlight that the Information Technology Act currently encompasses

[1] ProInd "Cyber Laws in India and Information Technology Act – All You Need to Know" pg.1 December 23, 2020.

all contemporary communication technologies.

According to the Act, a contract's acceptance can be stated electronically unless so agreed, and it will still be legitimate and enforceable. Also included in the Act's goals are the promotion and creation of a setting that is favourable for the deployment of e-commerce.

The IT Act 2000 was enacted to modernize outdated legislation and to enable better handling of cybercrimes. Although the term "digital signature" was defined in ITA-2000, the explanation was unable to account for all facets. As a result, the word "Electronic signature" was defined in ITA as a method of implementing signatures that is legally valid and which include digital signatures, biometric identification, and other types of electronic signatures. The term "communication devices," which included cell phones and other gadgets that could send any type of text, video, or audio, among other things, was included. The phrase "data theft" has taken the place of the word "hacking" in Section 66. The section addresses topics such sending insulting texts, falsifying message origins, identity and electronic signature theft.

Scope of ITA and Its Applicability

A change adopted in 2008 expanded the Information Technology Act-2000's scope and applicability. Aside from nations like the United States, Japan, Singapore, Malaysia, and others, India is the 12th nation in the world with cyber laws. The ITA-2000 offers legal guidelines that have an impact on information legally. Indian cyber laws offer a number of beneficial provisions from the perspective of Indian e-commerce. This statute established email as a legitimate form of communication that may be proven in court. Legal legitimacy was also granted to digital signatures. Corporate entities now have access to the necessary remedies.

The Important Provisions of IT Act

The Information Technology Act is a significant part of the overall Indian legal system since it governs how cybercrimes are investigated and prosecuted. The relevant sections are as follows:

Section 43: The section of IT Act is applicable to those who commit cybercrimes, such as harming the victim's computer without the victim's consent. If computer gets damaged in such case without owner's permission, the owner is completely entitled to receive a refund for entire damage.

Rajesh Aggarwal of Maharashtra's Information Technology department, who served as the case's representative, ordered Punjab National Bank to compensate Rs 45 lakh to Manmohan Singh Matharu, the MD of Pune-based company Poona Auto Ancillaries, in *Poona Auto Ancillaries Pvt. Ltd., Pune v. Punjab National Bank, HO New Delhi & Others (2018).* In one instance, a fraudster used Matharu's account at PNB, Pune, to transfer Rs 80.10 lakh after the latter responded to a phishing email. The complainant was requested to bear the liability because they opened the phishing email. However, it was determined that bank was incompetent because no security measures were made against accounts that had been formed fraudulently in order to mislead the complainant.

Section 66: Any fraudulent or dishonest behaviour covered by Section 43 is addressed by Section 66. In such cases, the maximum penalty is three years in prison or a monetary fine of Rupees 5 lakh.

In *Kumar v. Whiteley (1991)*, the accused acquired illegal access to Joint Academic Network (JANET) throughout the process of investigation and modified, added, and removed files. Investigations revealed that Kumar had been accessing BSNL broadband Internet connections under the guise of a valid authenticated person and altering computer records relevant to subscribers' broadband Web user accounts. The CBI launched an inquiry into Kumar after discovering unlawful utilisation of broadband Internet on his computer, which was the foundation of an unidentified allegation. The subscribers also lost Rs 38,248 as a result of Kumar's wrongdoing. The Additional Chief Metropolitan Magistrate condemned N G Arun Kumar.

Section 66B: This section confirms a potential three-year jail penalty for obtaining computers or other communication equipment that have been illegally reported stolen. A fine of amount of Rs. 1 lakh might be levied, depending on severity. A fine of amount of Rs. 1 lakh might be levied, depending on severity.

Section 66 C: Password hacking, digital signatures, and other types of identity theft are the main topics of Section 66C. This section carries a fine of one lakh rupees and a maximum sentence of three years in prison.

Section 66D: This section discusses computing assets personation cheating. If found to be guilty, the penalty carries a maximum three-year prison sentence as well as a maximum fine of Rs. 1 lakh.

Section 66E: According to the section, it is illegal to take images of private spaces and publish or transmit them without the subject's permission. If proven guilty, penalties include a maximum of three years in prison and/ or a fine of Rs 2 lakh.

Section 66F: Terrorism committed online. If found liable for a crime, a person could spend the rest of their life in prison. As an illustration, consider the time when an email threat was issued to National Stock Exchange and the Bombay Stock Exchange, challenging the security authorities to thwart the terror attack plot against these institutions. The offender was captured and charged in pursuance of Section 66F of the Information Technology Act.

Section 67: This deals with posting coarse language online. If found guilty, the maximum prison sentence is five years, and the maximum fine is Rs. 10 lakhs.

The Advantages and Disadvantages to the IT Act

The following advantages of this regulation include:

- Because of the Act, numerous businesses can now perform e-commerce with no worry. Until recently, our nation's expansion of e- commerce was stifled by the absence of a legal framework to regulate online business dealings.
- Corporations can now execute online transactions using digital signatures. The Act formally recognizes and approves digital signatures.
- The Act also makes it possible for even corporate entities to function as Certification Authorities for the purpose of issuing Digital Signature Certificates in accordance with the Act. The Act makes no distinctions regarding the type of legal body that may be chosen to serve as Certifying Authority, so long

as the requirements set forth by the government are met.

- Additionally, it offers details on the security issues that are extremely critical for the success of using electronic transactions. Secure digital signatures, that had to be subjected to a system of a guarantee and insurance product, were described and approved as part of Act. Consequently, it is reasonable to conclude that digital signatures now are safe and will have a significant economic impact. Digital signatures can aid in securing online transactions.

Hacking of corporate systems and data is a widespread occurrence. However, the IT Act significantly altered the environment. Corporate companies now have a legal recourse available to them if someone accesses their computers or network and modifies or copies data. Anyone who utilizes a computer, computer program, or computer network without owner's or another responsible party's consent is subject to damages.

However, the aforementioned Act has certain issues.

- As Section 66A doesn't really define the expression "offensive" and "menacing," it is deemed to be in compliance with Article 19(2) of Indian Constitution. It was unclear whether these concepts encompassed morals, incitement, public order, or defamation. As a result, these expressions are ambiguous.
- The Act hasn't addressed crucial problems like encryption and content regulations, which are especially important given how susceptible the internet is.
- A domain name also isn't covered by the Act's purview. The law doesn't really define domain names and doesn't outline the rights and obligations of domain name owners.
- The Act does not contain any language addressing domain name owners' Intellectual Property Rights. Important copyright, trademark, and patent-related issues were not addressed in the aforementioned law, which led to several loopholes.

Issues Not Addressed by the ITA

Although this Act offers a number of benefits, it is nevertheless insufficient and has a number of flaws, some of which are:

1. The law makes no reference to intellectual property rights. There aren't regulations or provisions governing copyright, trade mark, or the patent of electronic records, or relating to domain name holders.
2. No policies pertaining to the subject of online payment gateways are mentioned.
3. The act gives the Deputy Superintendent of Police complete investigative authority over cybercrime matters, therefore corporate entities are unable to avoid the DSP's wrath.

THE NATIONAL CYBER SECURITY POLICY OF 2013:

The 2013 Cyber Security strategy sought to provide a safe online environment for individuals, businesses, and the government. These were the main goals of this policy:

1. To provide a safe online environment that safeguards data and information infrastructures and increases public confidence in the IT industry.
2. To strengthen collaboration and create successful public-private partnerships and public-private interactions by working together technically.
3. To establish the body for certification and inspection of all such products and to increase the visibility and authenticity of ICT products, by creating a workforce of around 500,000 trained cyber security specialists within the next five years.
4. To safeguard information during the time it is processed, stored, or sent to preserve citizens' privacy and limit financial damages.

THE INDIAN PENAL CODE 1860

The following sections of IPC may be used by agencies of law enforcement, if the IT Act is insufficient to address particular cybercrimes:

- Section 292: Originally intended to handle the sales of pornographic materials, this had developed in the digital world to also cover different cyber offences. This clause also applies to how pornographic or sexually suggestive activities or excursions of youngsters are publicized or distributed electronically. Such offenses are punishable by up to two years in jail and fines of Rs. 2000. For persistent (second-time) offenders, any of the aforementioned crimes may result in a sentence of a maximum of five years in prison and a penalty of up to Rs. 5000.
- Section 354C: According to this law, photographing or publishing images of a woman's privates or intimate acts without her agreement constitutes cybercrime. Voyeurism is the only topic that this section discusses because it is illegal to watch a woman engage in sexual activity. Sections 292 of IPC and Section 66E of IT Act are broad enough to include offenses of a similar character in the absence of this section's essential components. First-time offenders may receive a sentence of up to three years in jail, while repeat offenders may receive a sentence of up to seven years.
- Section 354D: This chapter describes and penalizes stalking, including both physical and online stalking. Cyberstalking is the practice of following a woman through technology, such as the internet or email, or contacting her despite her lack of interest. For the first offense, this crime carries a maximum sentence of 3 years in prison; for the second offense, it carries a maximum sentence of 5 years in imprisonment and a fine.

A victim in the 2017 case *Kalandi Charan Lenka v. the State of Odisha* suffered reputational injury after receiving a string of vulgar messages from an unidentified caller. Additionally, the accused sent out the victim emails and made a false Facebook account with modified pictures of her. Due to this, the High Court found the accused initially responsible for several offences of cyberstalking under the IT Act and IPC Section 354D.

- Section 379: The maximum sentence under this section for stealing is three years of incarceration in addition to the fine. The IPC Section is relevant inter alia because several cyber-crimes include stolen computers, data, or electronic equipment.

- Section 420: In this section, it is discussed how to induce the delivery of property dishonestly and through deceit. Under this clause, cybercriminals who commit offenses including fabricating websites and conducting online fraud face a seven-year prison sentence in addition to a fine. This part of the IPC deals with offenses including creating phony websites or stealing passwords for financial gain.
- Section 463: This section deals with electronically fabricating documents or records. Under this clause, spoofing emails is penalized by a maximum of seven years in imprisonment and/or a fine.
- Section 465: This clause usually discusses how forgery is punished. Under this provision, offenses including email spoofing and creating fraudulent papers online are dealt with and penalized with up to two years imprisonment, fines, or both. In the 2005 case of Anil Kumar Srivastava v. Addl. Director, MHFW, the petitioner had falsely signed an AD's signature and afterwards filed a complaint that contained untrue accusations against the same person. The Court determined that the petitioner was accountable under Sections 465 and 471 of the IPC since he also tried to pass onto it as a legitimate document.
- Section 468: A seven-year prison term and a fine may be imposed for fraud committed with the purpose to defraud. Email spoofing is also prohibited by this provision.

In addition to the statutes mentioned above, there are numerous other parts of the Indian Penal Code and the IT Act that deal with cybercrimes.

Even if there are laws in place to combat it, the prevalence of cybercrime is still sharply increasing. According to reports, there were only 50,000 documented occurrences of cybercrime in India in 2020, a rise of 11.8% from the previous year. Owing to the underreporting, the jurisdiction of crime, public ignorance, and the rising costs of investigations due to technology, cybercrime is one of the hardest offences for the police to resolve.

Due to overlapping between the provisions of the IPC and IT Act, certain offenses may wind up being bailable under IPC but not pursuant to the IT Act and vice versa, or perhaps compoundable under IPC but not under IT Act and vice versa. For instance, if the behaviour involves hacking or data theft, the offenses under sections 43 and 66 of Information Technology Act are both bailable and amendable, in contrast to the offenses under Sections 378 and 425 of IPC, which are neither bailable nor amendable. In addition, if the crime involved receiving stolen property, section 66B of IT Act applied instead of section 411 of the IPC, which did not allow for bail. In a similar vein, under Sections 66C and 66D of the IT Act, the crimes of identity theft and defrauding by personation are punishable by a combination of fines and time behind bars, although they are not for crimes under sections 463, 465, and 468 of the IPC and are not subject to bail.

The Bombay High Court examined the dispute between offenses that are not bailable and not compoundable under Sections 408 and 420 of the IPC and those that are under Sections 43, 65, and 66 of the IT Act in Gagan Harsh Sharma v. The State of Maharashtra (2018).

COMPANIES ACT, 2013

According to the vast bulk of corporate stakeholders, the Companies Act of 2013 is the most important legal need for effectively managing everyday operations. This Act codifies the necessary techno-legal requirements, posing a challenge to noncompliant businesses by putting the legislation into effect. The SFIO (Major Fraud Investigation Office) is given authority to look into and prosecute severe frauds perpetrated by Indian firms and their directors as part of the Companies Act 2013 (Act).

The Companies Examination, Investments, and Inquiry Rules, 2014 announcement has caused the SFIOs to take this matter even more seriously and pro-actively. The legislation made sure that every component of cyber forensics, e-discovery, and cyber-security assessment is sufficiently addressed by making sure that almost all regulatory codes and standards are properly covered. Additionally, the Companies (Management and Administration) Rules, 2014 establish a stringent set of regulations that affirm the cybersecurity duties and responsibilities of company executives and directors.

The National Institute of Standards and Technology (NIST) has certified the Cybersecurity Framework (NCFS) as a framework for harmonizing the cybersecurity approach, making it the most reliable global certification organization. The NIST Cybersecurity Framework offers best practices, standards, and guidance for managing cyber-related risks. This framework places the highest priority on flexibility and affordability. Additionally, it intends to promote resilience and safeguard crucial infrastructure by putting the following measures in place:

(i) Improved knowledge of, control of, and mitigation of cybersecurity threats.
(ii) Avoid data loss, unauthorized use, and restoration expenses.
(iii) Choose the operations and activities that require security the most.
(iv) Demonstrates the reliability of the companies that guard important assets.
(v) Prioritize investments to maximize the cybersecurity return on investment (ROI).
(vi) Complies with contractual and statutory requirements
(vii) Helps the larger information security program.

The process of managing cybersecurity risk is made simpler when ISO/IEC 27001 and the NIST CSF framework are used together. Additionally, NIST's cybersecurity guideline makes it simpler to collaborate within organizations and throughout the supply chain, facilitating more efficient communication.

Why Indian laws against cybercrime

Our nation, like the others, is excessively concerned about cyber security and related crimes. India in particular is facing an increasing number of cyber security issues, and it must take decisive action to address them. According to a recent Economic Times research of cybercrime, the government is losing close to R. 1.25 lakh crore year due to cyberattacks.

Another analysis conducted by Kaspersky found that between the beginning of 2020 and the end of that quarter, the number of attacks in India grew from 1.3 million to 3.3 million. India recorded the most attacks ever in July 2020, totalling 4.5 million, making it the highest amount ever. In July 2021, Mastercard Asia/Pacific Pte Ltd (Mastercard) was prohibited from bringing onboard new domestic clients because it had violated Reserve Bank of India guidelines regarding the preservation of payment system data.

However, a cyber security policy is insufficient to address the risks created by the internet, and training is the most efficient way to deal with these dangers. The government must allocate enormous resources to protecting crucial data assets. To reflect the most recent advancements in law and technology and to address the problems brought on by the quickening pace of technological change, cyberlaw must be updated.

Importance of Cybercrime Laws

The significance of cyber laws can be illustrated by the following examples:

- To prosecute people who engage in illicit online activity is a key objective of any cyber law. Cyber laws are necessary in order to properly prosecute crimes of this nature, including cyber abuse, attacks on other websites or people, record theft, disruption of every company's online workflow, and other criminal actions.
- When a person violates a cyber law, action is taken against them based on where they are located and how they were involved in the offense.
- The most crucial issue is to prosecute or exonerate hackers because most cybercrimes go outside the purview of criminal charges, which are not crimes.
- The usage of the internet is also accompanied by security worries, and there are even some evil people who wish to get unauthorized access to the computer system and use it to perpetrate fraud in the future. Therefore, all regulations and cyberlaws are created to safeguard online organizations and consumers from unauthorized intrusions and dangerous cyberattacks. There are numerous ways for people or organizations to take legal action against people who commit crimes or violate internet laws.

Need for Cyber Crime Laws in India

In nations like India, where the internet is widely utilized, cyberlaw is especially crucial. The law was passed in order to safeguard both persons and organizations against cybercrime. The cyberlaw gives other people or organizations the ability to file a lawsuit against someone who disobeys and breaks the law.

There may be a need for cyberlaw in the following situations:

- Everyone engaged in stock transactions is now protected by cyber law in the case of any fraudulent activities because all stock transactions are now completed in demat format.
- The majority of Indian businesses use electronic records. This law might be required by a business to stop the misuse of such data.
- Many government documents, including income tax returns and service tax returns, are now filled out electronically as a result of the quick growth of technology. By hacking into government portal websites, anyone can misuse those forms, hence cyberlaw is necessary in order to pursue legal action.
- Electronic contracts and digital signatures are frequently used in business transactions. Anyone participating in them can readily make advantage of digital signatures and electronic contracts improperly. Cyberlaw offers defence against these kinds of frauds.
- Today, debit and credit cards are used for shopping. These credit and debit cards are unfortunately

duplicated by certain online scammers. A method that enables someone to acquire your information online is the cloning of a credit or debit card. Cyberlaw can preclude this as Section 66C of the IT Act stipulates a 3-year prison sentence and a fine of up to one lakh rupees for anyone found using an electronic password dishonestly or fraudulently.

Security and Cyber Crime

Cybersecurity is the grouping of technologies, procedures, and procedures used to guard against attacks, damage, and illegal access to networks, devices, programs, and data. Information technology security is an alternative name for cyber security.

Computers and other equipment are used by a variety of organizations, including the government, the military, businesses, financial institutions, and healthcare facilities to process and store incredibly huge volumes of data. Numerous of those documents contain sensitive information, such as intellectual property, financial data, personal data, etc., to which unauthorized access or disclosure may have unfavourable effects. Protecting the systems used by businesses to process and store sensitive data sent via networks and to other devices is a developing field of cyber security. Therefore, cybersecurity is the field devoted to protecting both the means via which such sensitive information is communicated or kept as well as the sensitive information itself. Companies and organizations, particularly those entrusted with safeguarding confidential data (including attacks pertaining to national security, health information, or financial information), must take steps to safeguard the safety of their proprietary business and personnel data as the numbers of cyber-attacks and the complexity of those attacks rise.

Cybersecurity Tactics

It is also critical for a company to establish and implement an effective cybersecurity strategy. Cybersecurity plans must incorporate the following elements:

Ecosystem: In order to prevent cybercrime, an organization's ecosystem must be strong. In general, an organization's ecosystem consists of three components: automation, interoperability, and authentication. By creating a secure and robust system, the organization will be able to protect these components against viruses, attrition, hacks, insider assaults, and equipment theft.

Framework:

A framework for complying with security requirements is an assurance that such standards will be followed. As a result, infrastructure updates are conceivable. It also makes collaboration between companies and governments easier.

Open standards:

Open standards: Businesses and individuals can simply implement appropriate security measures owing to open standards. These standards will also enable better economic growth and a wider spectrum of innovative technology.

IT mechanisms:

There are numerous IT measures or techniques that can be advantageous. It is critical to promote these tools and mechanisms in the battle against cybercrime. Among the measures are end-to-end protections, association-based protection, link-based protection, and data encryption.

E-governance:

The government can give services online through e-governance. However, e-governance is not widely used in several countries. Cyberlaw should prioritize the advancement of technology in order to give citizens more authority.

Infrastructure:

One of the most important tasks in cybersecurity is to secure the infrastructure. This is particularly true for the electrical grid and data transmission networks. Cybercrime is frequently committed against outdated infrastructure.

Difference between Cybercrime and Cybersecurity

Cybersecurity is more than just a collection of recommendations and measures to prevent cybercrime. Finally, cyber-security attempts to make life tough for hackers by preventing them from discovering and exploiting weaknesses in government and corporate networks. In contrast to traditional crime, cybercrime focuses on protecting the privacy of individuals and their families while conducting online activities.

Following is a list of distinctions between cyber security and cybercrime that you should be aware of:

1. Types of crime: Cyber security crimes are those in which a computer program, hardware or computer network is the primary target of a cyberattack if it is compromised. Cybercrime, on the other hand, is associated with a particular person or group of persons, as well as their data, as the major targets.
2. Victims: Second, there are distinctions between the categories of victims within these two domains. In cyber security, governments and companies are the principal targets, whereas victims in cybercrime might include individuals, families, enterprises, governments, and organizations.
3. Subject matter: Both of these subjects are explored in distinct disciplines. Cybersecurity is a subset of computer science, information technology, and computer engineering. To improve network security, code development, networking, and engineering are employed. Cybercrime, to the contrary hand, comes into the psychological, criminological, and social categories. It describes a theory that explains how crime occurs and suggests how it can be avoided.

CYBER LAW IN U.S.A.

Cyber laws are enacted in United States on both a Federal and State level. The division of powers between these two distinct levels is subject to specific rules.

Scope and Its Applicability

The laws governing cyberspace in the United States include reference to numerous categories of cybercrimes. Getting illegal access of government computer also obtaining sensitive data, damaging a computer with a malicious application or gaining unauthorized access, harming a system to reap financial rewards, etc. are all regarded crimes. There's no requirement that laws be universal or consistent among the 50 states; each one is allowed to establish its own legislative bodies. To ensure uniformity in the law, private organisations prepared some enactments such as the Model Penal Code and Restatements, which were then given to States for adoption.

CYBER CRIME LAW IN EUROPE

The Council of Europe was founded in 1949 with the purpose of supporting democracy, human rights, and the rule of law throughout Europe. It is made up of all 43 states that make up the European Unions.

EVALUATION, FINDINGS, AND DISCUSSION

The right requirement for Indian law can be assessed by comparing it to the legal systems of developed countries. Data, do not all have the same needs or relevance; rather, their utility varies. As in the US, we must therefore establish several categories of data with varying degrees of relevance. Additionally, the requirements of the IT Act deal primarily with data extraction, data destruction, etc. Because IT Acts do not provide complete data protection for businesses, private businesses were ultimately had to go into privately - held contracts in in order to safeguard their data. These agreements apply in the same way as a general contract. Our legislators left some gaps in the 2006 bill's design despite efforts to create a separate discipline for data protection laws. While today's requirements call for comprehensive Act, the measure was entirely crafted using the format of UK Data Protection Act. It can therefore be inferred that a prepared draft of data protection law based on US regulations would likely be more accommodating to present needs.

CONCLUSION

As technology advances, strange components that are alarming are appearing on the dark web. The Internet has evolved into a weapon for evil activities, which intelligent people use for ill purposes and occasionally for financial benefit. Thus, at this point, cyber laws enter the picture and are critical for all citizens. Because cyberspace is such a tough territory to navigate, some acts are classed as grey activities that are not authorized by law.

To keep up with the rising dependency of humans on technology, cyber laws in India and around the world must be constantly updated and refined. As a result of the epidemic, it has also resulted in a large growth in the number of remote employees, which has raised the demand for application security. Legislators must take extra precautions to stay ahead of imposters and act against them as soon as they appear. It can be avoided if lawmakers, internet service providers, banks, e - stores, and other intermediaries collaborate. However, it is completely up to users to take part in the fight against cybercrime. The one and only way for online safety and resilience to flourish is for these stakeholders' actions to be scrutinized to ensure they remain within the bounds of cyberspace law.

Trolling, child pornography, harassment, phishing frauds, cyber stalking, and denial-of-service assaults are just a few of the actions that fall under the category of "cybercrimes," where computer is either the aim, the tool, or even both. Governments all around the world are pursuing a variety of measures to combat cyber-crimes, but opponents of cyberlaw caution the authorities about the negative effects of excessive online activism. Some researchers have asserted that government regulations make it more difficult for them to identify weaknesses in Internet infrastructure.

Computers, Internet and networks constitute the technical foundation of cybercrime worldwide, therefore all countries experience the same types of cybercrime. This necessitates that nations work together internationally to combat cybercrime. Every aspect of electronic commerce, as well as online transactions and other online activities, are covered by cyber laws from a legal standpoint.

Because people have become more reliant upon the Internet, criminal activity will likewise continue to rise. The nation's legislative authorities should continually be aware of how quickly cybercrimes are developing, and their laws ought to be capable of minimizing them as much as feasible. Therefore, it is the obligation of both the government and law makers to ensure that all perspectives and issues relating to cybercrimes have been taken into consideration in order for the laws to continuously and actively develop in this area.

REFERENCE

Articles and Books

1. Business Standard, "Emerging Global cyber Law Trends 2014" Last accessed: April 2016.
2. Mondaq, "Cyberlaws: An Indian perspective", Last accessed: January, 2015.
3. Cyber Laws India.net , "Cyber laws in India", Last accessed: April 2016.
4. Information Security Awareness, "Cyber Laws of India", Last accessed: April 2016.
5. "The Information technology (Amendment) Bill 2008", Government of India, December 2008.
6. "National Cyber Security Policy-2013", Ministry of Information and Communication Technology, July, 2013
7. S. W. Brenner, "State Cybercrime Legislation in the United States of America: A Survey", Last accessed: January, 2015
8. M. Dekker, C. Karsberg, B. Daskala, "Cyber incident reporting in EU", European Network and Infor-

mation security agency, August, 2012.

Websites

1. https://probono-india.in/blog-detail.php?id=218
2. https://www.appknox.com/blog/cybersecurity-laws-in-india
3. https://www.myadvo.in/blog/what-is-the-cyber-law-in-india/
4. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/
5. https://blog.ipleaders.in/cyber-crime-and-cyber-security-an-overview/#Relation_between_Cyber_Crime_and_Cyber_Security
6. https://digitalguardian.com/blog/what-cyber-security
7. http://www.proind.in/blog/cyber-laws-in-india-and-information-technology-act-all-you-need-to-know/
8. http://www.bhagininiveditacollege.in/cgi-sys/suspendedpage.cgi
9. http://www.business-standard.com/article/technology/emerging-global-cyberlaw-trends-in-2014-115010500301_1.html
10. http://www.mondaq.com/india/x/257328/Data+Protection+Privacy/An+Overview+Of+Cyber-Laws+vs+Cyber+Crimes+In+Indian+Perspective
11. http://www.cyberlawsindia.net/cyber-india.html
12. Available at: infosecawareness.in/cyber-laws
13. http://jolt.richmond.edu/v7i3/article2.html

Statutes

1. Information Technology Act, 2000
2. Indian Penal Code, 1860
3. Indian Evidence Act, 1872
4. Banker's Book Evidence Act, 1891
5. Reserve Bank of India Act, 1934
6. Companies Act, 2013

Cases

1. *Poona Auto Ancillaries Pvt. Ltd., Pune v. Punjab National Bank, HO New Delhi & Others AIR 2018*
2. *Kumar v. Whiteley AIR 1991*
3. *Kalandi Charan Lenka v. the State of Odisha* AIR *2017*
4. *Anil Kumar Srivastava v. Addl. Director, MHFW AIR 2005*
5. *Gagan Harsh Sharma v. The State of Maharashtra AIR 2018*

22

POLICIES, LAWS AND REMEDIAL MEASURES STRENGTHENING THE FIGHT TO CYBER TERRORISM IN INDIA

KEYWORDS

CYBER TERRORISM, INTERNATIONAL DE DROIT PANEL

CHAPTER TWENTY TWO

POLICIES, LAWS AND REMEDIAL MEASURES STRENGTHENING THE FIGHT TO CYBER TERRORISM IN INDIA

AUTHORS

SANGHAPRIYA RAY, RESEARCH SCHOLAR, SHARDA UNIVERSITY, GREATER NOIDA, UTTAR PRADESH, INDIA

PRANJAL TIWARI, STUDENT (BALLB), SHARDA UNIVERSITY, GREATER NOIDA, UTTAR PRADESH, INDIA

DR. ROHIN KOUL, ASSISTANT PROFESSOR, SHARDA UNIVERSITY, GREATER NOIDA, UTTAR PRADESH, INDIA

ABSTRACT

This digital span, with an abundance of technological advancements had eased our lives to a very large extent. A space had been provided to all the individuals to express their ideas in this digital world, and hence it came to be recognized as cyberspace. However, a coin always has two faces and thus, at one hand where this technology has eased our lives, on the other hand there are some people on this platform too, which tries to take benefit of the vulnerable sections of the society. Cyber terrorism is one such weapon by which, such disturbing elements tries to take the advantage of the exclusive contents and information of the

people available on the cyberspace by using against them. The legislative authorities had time to time brought many laws to control such notorious elements, but these people are always two steps forward than these law makers. Thus it is a high time for the law makers to make such flexible policies both at the international as well as municipal level, such that,a security could be provided to the people with the least infringement to their privacy by the state.

The problem with the prevalent cyber laws is that very few of them focus on the aspect of cyber terrorism. Thus, via this research paper, we would try to evaluate the various statutory measures and policies which are present around the world, dealing the cyber terrorism, since this problem is something which common to all the nations.

INTRODUCTION

In this era of cyber technology in the 21st century could be determined as the modern industrial revolution, was highly motivated by the Internet and the set of connections computers gain posed a major threat to the humanity and the humanitarian needs. The new industrial revolution has brought upon with itself advanced crimes. Cyber terrorism could be determined as only one of its kind modes for cyber terrorists for major 3 criteria. First and the foremost the use of computers and other sources is quite a cost affordable source to do crime. Secondly, cyber-crime enhances the chances of the parties to get involved in the dangerous scenarios of crime. Thirdly, the criminals can use the cyber technology easily without being caught and the security agencies by no means are able to reach to them. The development of cyber technology has ultimately boosted life style for the world's economic sector to a much larger extent.

These new discoveries developed during the phase of the 21st century provides a boost to the development, and paved new pathways at the same time which positively gets the cause to be in favor of public through a choice of forms and make a payment to the different socio-legal such as employment, right to proper living wage and diversity in the company of others. Currently there is no unwillingness in the thought that in the region of information technology (IT) there has been a transformation of India's character as the comprehensive player under the global market in the sectors of modern information technology solutions and computer advancements. The development of political advancement has become possible due to the strategic reason of enlarging the use of information technology associated goods and services by the countries. We the people by our primitive habits, have a predetermined nature to return back to the evolution process of finding major inventions and technologies. The enhancement of modern technologies around us with superior chances has improved our standards of living via simplified and advanced technological devices. As there is development in time, the technological enhancements as well have an ability of being utilized in the form of a source destruction inside the palms of extremists.

CYBER TERRORISM – MEANING

By the enhancement of time human beings has focused more on the improvement and innovation, leading to a new habit and they began to learn the malicious usage of every computer associated goods and services. Similarly, it has been observed that the advancement which came up with the field of supercomputer and cyber technology improved lives by means of simplified, swift and better standard of life on the other hand one section utilized these technological developments additionally in order to strengthen the cyber terrorists to cause tremor in the world of information technology. By the enhancement of mankind it has been observed that slowly and steadily by becoming dependent on technology and networked systems, not all the people took part in genuine benefits which could have been derived from this trend, but at the same time the malicious groups, such as extremists, strategic crime panels, and the other terrorist groups by the use of cyber technology has caused destruction throughout the world.

EVOLUTION OF CYBER TERRORISM

Cyber terrorism can be defined as the use of information technology networks, along with the computer technology, as the source of destruction. Extremism via the cyber technology calls for in giving an extremist element which is ultimately determined as “cyber terrorism”. As a traditional purpose, the term ‘cyber terrorism’ came into usage in the1980s while Mr. Collin, who was a topmost researcher at the Information Science Institute (ISI) situated at California, framed this new technical term via the combination of two words which are cyber sector and terrorism.

Currently, after twenty years thereon, cyber-crime especially cyber terrorism has been labelled as a different aspect not merely taken as a plain, extensively simple definition. The reason behind such a rapid advancement is that at one hand we have various loopholes in the classification of a concrete definition of cyber terrorism as the word itself consists of ‘cyber’- an explanation through which mainly correlates of anything which is associated with computer - and ‘terrorism’- that has been, since the year of 1793, has come upon with more than two hundred explanations. ‘Cyber’ as a term could be determined as everything associated to cyber technology, currently, along with the other information technology systems. At the same time, one person’s terrorism may be a form of revolution for the others. Hence there is no any kind of astonishment as to how constantly the learned people and researchers had to revise with definition as to terrorism with the changing spans of time.

Technology cannot provide any kind of exactness of cyber terrorism in our society. Some kind of electronic mail hacking may be capable of conducting some kind of actions of normal procedure of hacking for some, and this might be as small in nature for someone that it could be hardly be a medium of cyber-crime for the other people. The term ‘cyber terrorism’ can be explained in a very narrower and in a very specific form. Cyber terrorism could be explained as tacking control of one’s system or dangerous attacks in the software against the operating devices, however the denotation of the terrorism related to computer systems in present era is quite associated to criminal proceedings such as sex trafficking or child pornography via the use Internet services. Another panicking situation arising around us which has been increasing among the users is that, they are becoming slaves to computer universe and thus are prone towards the attack by the cyber terrorist in our cyber world.

Past few years from today, during 1998, Ehud Tenenbaum, who was a young Israeli computer expert popularly known with the term 'Analyzer', intercepted through notebook computer devices used by the Pentagon, NASA and various more highly classified computer systems working in America. An American Defence computer expert called it "the large amount orderly and systematic lay into the Pentagon has seen to date". Such an advanced system of tracking business during those phases of time was very much associated as a set of a cipher terminology, the 'Solar Sunrise', which was coined as per the F.B.I. During the year 2001, a teenager of around 16 years of age residing in Canada, popularly known as 'Mafia Boy' in addition tried with an attempt of hacking down onto safety apparatus associated with certain kinds of the cyber security and confidential information in the U.S. Practically, cyber terrorism comprises of an in linked mainframe technology in order to conduct certain terrorist activity. Terrorist groups through means of the Internet had been conducting certain activities, such as contacting with each other, generating propaganda, tracking the intelligence strategies. With the utilization of the computer internet terrorists could easily communicate through each other: this is not under the supervision of any central control, it is further not eligible of being tracked down in order it to contain or restriction and it is open to everybody who requests to exploit it. However, the cyber-world can also be utilized in a much adverse way, not merely as an indirect tool for executing an attack, but in addition as a destruction weapon. One method to make use of the computer technology in cyberspace is through cyber attacks on websites. Sometimes, such attacks help in conducting fully planned attack over the India-Pakistan conflict associated with the territory of Kashmir, on the grounds of the conflict related to Israel and Palestine and towards the NATO cyberspaces at the time of attacks done on Kosovo under the initial phases of 1990's. All those activities are yet not considered under a category of "terrorism" in the good judgment that they did not seem to cause any kind physical or real hurt and are merely done to the regime, as provide under the explanation of the term terrorism explained via the Financing Convention.

The term cyber terrorism can possibly be considered as something which lies in between the terrorism and cyber crimes. These categories are moreover fairly modern concepts, along with other forms of cyber crimes. Some unique thing about the explanations of all such terms still needs some more focus. Focusing on cyber crimes generally, at one hand there are a number of breaking of the criminal conducts that utilizes the usage of computer systems along with other cyber technology apparatus, regularly conducted by the medium of internet, yet this need not to be done every time. In accordance with the terrorism, the United States leadership has come upon with many definitions, and internationally, throughout the world there has been no such kind of clarity over the explanation of terrorist activities. Extremist communities are utilizing the cyberspace in order to conduct a number of extremist purposes, such as communicating, creating propaganda, allotting sleeper cells and collecting intelligence. The exchange of ideas by the mean of computer related technologies are superlative for terrorists to communicate with each other freely: decentralization, the same could not be subjected to certain kinds of restriction and thus provides room for everyone in any manner who wants it as a medium of exploitation. At the same time, the internet platforms are utilized in an adverse manner, for merely being used as a medium of conducting any extremist activity. The various medium through which attacks by which computer related extremism is promoted is the absence of any small rules in order to restrict terrorism activities via the cyber space. Terrorism through cyberspace is extremist exploitation of cyber technologies with an aim of hurting the sentiments of the people or to conduct such kind of malicious activities with an approach that may try to spoil the human being life. Joel Trachtman "distinguishes between different kinds of networks that may be subjected to cyber terrorist attacks; armed and civilian defence networks; other law-making networks (police, fire); privately or in public owned networks second-hand to regulation free utilities and other systems for as long as infrastructural armed forces (electricity, water); and shared networks old by single patrons and businesses for communication, learning etc".

LAWS IN INDIA TO COUNTER CYBER TERRORISM

During the dialogue of the 2006 Bill, the eminence commission felt that enough attention was not particular to the conception of cyber crime and cyber terrorism in the anticipated amendments. The administrative area of in a row Technology (DIT) had full a survive that basic amendments bottle be agreed out in the accomplish which will be in air with the provisions of the Indian severe set of laws and Criminal process Code. The eminence Committee, in distinguish opined that the time deep-rooted punishing provisions in India are not enough to bear changes to incorporate cyber crime as a crime with custody for a longer time and with top fine. The eminence agency not compulsory that the DIT express stringent, great and satisfactory laws to reduce cyber terrorism in the country. It was brought to detect of the commission that a great deal required focus was not certain to the issue. of cyber terrorism in the 2006 Bill here was no free provision in the entirety of the in-rank Technology ham it up as the country was battling against' the shocking crime of terrorism during the Mumbai attacks of November 26, 2008. The ask put to the sector was if having any legislation industry with crimes like morphing, cyber terrorism and other down-to-earth cyber crimes carrying a punishment of with the chief select and term will aid limit the swell of such offences. The sector was of the view that morphing would nonetheless be enclosed under sections 43 and 66 of the in-Information Technology, (Amendment) Act, 2006.The region of in order Technology furthermore took the view that cyber terrorism must be completed an offence carrying a punishment of with internment for an expression of 10 being and with adequate in policy with section 120 B and Section 121 of the Indian penal Code. The Committee, however, prominent that the name 'cyber terrorism' had not been clear everywhere in the IT Act, 2000 or in the 2006 Bill.

Section 66 F. Punishment for Cyber Terrorism

(1) Whoever, -

(A) With intent to threaten the unity, integrity, safekeeping or dominion of India or to smack terror in the natives or any sector of the intimates by-

(i) Denying or produce the rebuttal of retrieve to any self-authoritative to gain access to supercomputer resource; or

(ii) Attempting to find out or entry a supercomputer reserve without consent or exceeding approved access; or

(iv) Introducing or causing to begin any supercomputer Contaminant;

and by process of such conduct causes or is prone to origin casualty or injuries to people or hurt to or destruction of acreage or disrupts or conscious that it is probable to origin hurt or disruption of materials or armed forces fundamental to the go of the area or adversely touch the significant in a row infrastructure individual.

(B) On purpose or intentionally penetrates or accesses a supercomputer store without authorization or exceeding legitimate access, and by method of such conduct obtains retrieve to information, numbers or central processing unit folder that is limited for reasons of the confidence of the ceremony or unknown relations; or any limited information, numbers or central processing unit database, with reasons to judge that such information, information or PC catalog therefore obtained may be old to begin or apt to initiate injury to the welfare of the power and integrity of India, the collateral of the State, pleasant relations with distant States, communal order, politesse or morality, or in next of kin to contempt of court, slander or encouragement to an offence, or to the plus of any overseas nation, party of folks or otherwise, commits the offence of cyber terrorism.

(2) Whoever commits or conspires to commit cyber terrorism shall be liable to be punished by with captivity which may broaden to sentence for life.

INTERNATIONAL CONVENTIONS TO TACKLE CYBER TERRORISM

1. International De Droit Ponel Conference in Germany (1992)

The correlation International de droit Ponel (ADIP) seized the collegiums on 'Computer Crime and Other Crimes against in rank Technology' in Wurzburg (Germany). It gives an account avowed that individual 5% computer crimes were mortal reported to police. The Factors contributing to non-disclosure of cyber-crimes, according to this report, were as follows:

(i) Operational hustle and cargo space role of CPU hardware makes criminal past time dreadfully challenging to detect;

(ii) The edict enforcement agencies are short technological expertise to sell with cyber crimes;

(iii) Victims of these crimes are themselves uncertain in coverage the crime to the keep watch over as they pick up needless aggravation and squander of time and currency in this unproductive endeavor;

(iv) The panic about of unfavorable exposure in addition dissuades the victim from publicity the crime; and

(v) Failure of goodwill, opens confidence, investor's reliance or embarrassment, and so on. Is additionally about of the factors in price for non-exposure of cyber crimes. Although, this summit become not exactly connected to the cyber terrorism, comparable the troubles discussed at that point have been unequivocally and in a roundabout way interrelated to the cyber threat. Therefore, the worldwide place has on the right track discussing terrorist countenance of the internet.

2. G-8 Hi-Tech Crime Working Group (1998)

In the day 1998, in March to foil and domination the hi-tech crime G-7 had full initiatives and the UK (United Kingdom) got here directly to combat cyber crimes. G-8 nations are the widely wide-spread set of producing countries inside the world. In December 1997 G-8 meeting changed into detained at headquarter of the integrity ministers of the G-8 countries. The lawyer of USA, Janet Reno believed "criminals not are labelled via nation-run obstacles…… if we're to shelve up with cyber crimes, we responsibility be triumphant mutually as in no manner before." the information alliance at large their sign up for the subsequent regions everywhere these most critical nations cover arranged to collaboration:

1. To assign quantity of suitably educated and equipped commandment enforcement personnel to look at high-tech crimes;
2. To sit up customs to persuade attacks on pc networks;
3. To prosecute criminals inside the country everywhere they're found, at what time expulsion is not possible;
4. To keep means substantiate on pc networks;
5. To re-study the above-board codes in apiece residents to make sure that proper crimes for processor damage burden are prescribed;
6. To assure that the language makes it less complicated to have a look at the crimes;
7. For cooperation with the categorised sector to boom new conduct to understand and take a look at mainframe crimes;
8. To multiply hard work to exercise new exchange of ideas technologies, such as, record teleconferencing to get hold of proof from witnesses in other nations.

3. Internet Treaty by Council of Europe (2001)

Since 1980's the convention of Europe had been functioning to adopt the on the rise intercontinental disquiet over the threats posed by hacking and other central processing unit associated crimes. The entire the constituent States of the board of Europe collectively resolved that global alliance to eliminate cyber crimes essential be genuine, mutual and supportive in request to get together the ultimate goal of tackling the crisis of exposure of internet infrastructure. According to congress of Europe, nearby are next three key challenges in maintaining internet security:

1. Professional challenges that obstruct the aptitude of directive enforcement agencies to locate and prosecute cyber criminals that conduct online
2. Necessary for an exchange in one substantive and routine laws that retain not reserved lick with the shifting technology, creating officially authorized challenges to real prosecution of criminals in commission in cyberspace
3. Infrastructural desires to enhance the capability and knack of edict enforcement agencies to adhere to

stride with altering technology with prominence on instruction the group to wrestle cyber criminality. A new internet treaty was contemplated by the convention of Europe44 in 1997 which was enforced in the development of an article in 2001. The treaty hunted to contain internet crimes by requiring participating Nations to construct a feature equal mass of laws to covenant with illegal access, internet frauds and forgery, childish person pornography, copyright infringements etc. The treaty of board of Europe not compulsory procedures which may possibly management cyber crime behavior at the overall level. The treaty became at liberty 'worldwide custom on cyber crime' and it becomes alert on the next three chief issues:

- Organization of national laws, which defines cyber crimes
- Laying down stated research and prosecution methods to get through up with overall networks
- Putting in of a hurried and in impact system of intercontinental cooperation for warfare cyber illegal activity.

REQUIREMENT OF AN UPDATED ANTI CYBER TERRORISM POLICY IN INDIA

As in a very good variety of the international locations round the world, the cyber refuge scenario in India is considered one of relative mess and a figure of diffidence arising out of the periodic records of cyber espionage, cyber terrorism, cyber rivalry and cyber crime. The intricacy of the come forth has resulted in a digital paralysis. Formally authorized and regulation enforcement mechanisms take part in now not shifted gears rapidly as an awful lot as necessary to come to grips with growing cyber crime. Periodic newspaper hearsay trace at that a numerous variety of defensive activities is mortal pondered via collection of organizations, however that is all. Therefore, a coherent cyber self- belief certificates will without a doubt interfere with India's inhabitant sanctuary and financial improvement. It is essential that new hobby on the pinnacle ranges is compensated to ensuring that cyber-related vulnerabilities which might be able to collision on risky sectors are identified and removed. A coherent and all-inclusive cyber self-assurance guideline will give beginning to some of principal elements, together with genuine conceptualization of cyberspace threats; production of sturdy our on-line world thru a variety of measures, together with procedural criminal, diplomatic, global cooperation; foundation of desirable organizational structures; intensification of human resource development; and implementation of maximum super practices and guidelines. India's make contact with to cyber self-assurance has consequently afar been trailering hoc and piecemeal. A quantity of corporations performs been usual however their fastidious roles incorporate not been clean nor has synergy been fashioned surrounded through them. As it transcends a measureless domain, this cataract in the charter of the NSCS. However, at hand appears to be no institutional configure for implementation of guidelines. Neither the reserved region nor path has been proficient to construct in a row structure that realize how to be defined as exceedingly sturdy close to has not been enough philosophy on the implications of cyber battle. Meanwhile, masses of nations are gravely engaged in attendance to their cyber precautions doctrines and techniques. America, Russia, United Kingdom, France, Australia, Germany, New Zealand, South Korea, China, Brazil, South Africa, Denmark, Sweden, Singapore, Malaysia the report is protracted and developing are actively engaged in making sure a now not dangerous and get hold of cyber environment for their residents. The intercontinental population is and engaged in quite number discussions. NATO has completed the duty of creating cyber safekeeping institutions in organ nations. A put together of law-making specialists (GGE), level installation by using the un table general, gave a story in 2010 on "'trends inside the subject matter of ICT inside the historical past of international safety". The document close by became developing prove that states were emergent ICT as "gadgets of preventing and intelligence, and for biased functions". To confront challenges in cyberspace, the GGE not compulsory cooperation within the middle of minded companions, collectively with states, among states, and between states and civil the higher crust and the private sectors. The define cyber protection measures guiding precept text placed out by means of the DIT for within the public domain debate is an critical rung however it is largely a departmental attempt, now not delightful a entirety of governmental approach. DIT does not enjoy rule over departments.

CONCLUSION

The life of data in the authentic earth and the virtual planet is different. This discrepancy is conspicuous in each and every one the stages of signal detection, gathering, luggage compartment and exhibition before the court. The precarious segment is that altogether the investigation powers that be that are to blame true from the leg of crew of the support to the presentation of the substantiation before the invite requirement know the distinguishing attributes of the proof as a result that they canister defend the mark together by them. In this bear in mind the character of the courts plus will become most important because the courts be obliged to moreover be inside the vicinity to be pleased about the mainframe make clean untaken earlier than them. Contrary to the honest globe crimes someplace any cloth mark in the foci of name prints, bludgeon of crime, blood blemish lettering and all that tin be traced, inside the digital humanity such traces grow to be in particular stubborn to find. The science of supercomputer forensics is in advance import in the research departments, company global, control departments and many others. Conform to us appreciate approximately of the challenges which are complex within the sea to of cyber help detection, collecting, luggage compartment and exhibition before the court." it's far measured checking out to go out the facts from the supercomputer system is inside the foremost contemplated. This preserve be prepared with the consolation of computer forensics who are gifted to arrange display or equal make progress facts which may additionally enjoy been deleted intentionally. It is of the essence that the sufferer conveys the act enforcement agencies about the crime as untimely as feasible." the kind out of defense of cyber crime sign falsehood inside the indulgence of an effective and conversant mainframe forensics authority for the purpose that any inaccuracy inside the way be able to head to minuscule fee of the evidence. The mainly repeatedly faced obstacle is that the victim-companies are added upset with refurbishment of their systems to detailed operational grade noticeably than allowing identifiable demonstrate collection.

REFERENCES

1. Talat Fatima, *Cybercrimes*, p. 51, Eastern Book Company, Lucknow, 2011.

2. "*Sector Profile, Information Technology", India*, p. 1. Available on http://www.ficci.com /sector/21/ Project_docs/FICCI_website_content_-IT.pdf. Retrieved on 3 March 2014.

3. Aviv Cohen*, "Cyberterrorism: Are We Legally Ready?"* p. 1, Journal of International Business and Law, Volume 9, Issue 1 2010. Available on http://scholarlycommons.law.

4. Dev Kristula, *The History of Internet*, March 1997, Updated - August 2001, Available on http://www.davesite.com/webstation/net-history5.shtml?, Retrieved on 30 March 2013. Salaheddin J. Juneidi, *"Council of Europe Convention on Cyber Crime"*, p. 1, paper presented in 5th European Intensive Programme on Information and Communication Technologies Security (IPICS), 2002.

5. Albert Marcella & Greenfield, *Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes*, p. 205, 2nd ed., Auerbach Publications, Taylor & Francis Group,UK, 2007.

6. R.K. Tivari, P.K. Shastri and K.V. Shankar*, Computer Crimes and Computer Forensics*, pp. 278-9, Select Publishers, 2002.

7. John R. Vacca, *Computer Forensics- Computer Crime Scene Investigation, p.14, Vol. 1,* Charles River Media, UK, 2005.

23

CHALLENGES OF COPYRIGHT AND CYBER SPACE

KEYWORDS

INTELLECTUAL PROPERTY RIGHT , CYBER SPACE, COPYRIGHTS, INFRINGEMENT OF COPYRIGHT, IPC

CHAPTER TWENTY THREE

CHALLENGES OF COPYRIGHT AND CYBER SPACE

AUTHORS

SANIA DUA, LL.M STUDENT (CORPORATE AND COMMERCIAL LAW), SCHOOL OF LAW, SHARDA UNIVERSITY, INDIA

DR RITU GAUTAM, ASSISTANT PROFESSOR, SCHOOL OF LAW, SHARDA UNIVERSITY, INDIA

ABSTRACT

This paper aims to analyze challenges of copyright and cyber space. The paper is discussing the points of view in relation to the positive and negative impacts of the intellectual property systems. It brings also into discussion to infringement of copyright in cyberspace in national and international sense. Loop holes and recommendations in comparison of Indian copyright laws to developed countries laws.

INTRODUCTION

Copyright is a key issue in Intellectual Property Rights (I.P.R) in digital era. Though the term “Copyright” is not new, the modern technology brought in a great importance to intellectual property and copyright in particular, which has cropped up in new concepts such as computer programs, computer database, computer layouts, websites etc. A great care is taken to trace out the linkage between copyright and cyberspace, by taking the readers to have glimpses of database history, software nuances, which establish a ground reality upon this topic and clinches the issues with no iota of doubts anymore.

The internet has now become all encompassing; it touches the lives of every human being. We cannot undermine the benefits of internet; however, its anonymous nature allows miscreants to indulge in various cybercrimes.

Cyberspace can be defined as an intricate environment that involves interactions between people, software and services. It is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It’s also known as information technology security or electronic information security. The term applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories.

Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It’s also known as information technology security or electronic information security. The term applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories.

CHALLENGES OF COPYRIGHT AND CYBER SPACE

Cyber security denotes the technologies and procedures intended to safeguard computer networks and data from unlawful admittance of weaknesses and attacks transported through the internet by cyber delinquents.

Intellectual property refers to creations of the human mind, for example; a story, a song, a painting, a design, a program etc. The facets of intellectual property that relates to cyberspace are covered by cyber law namely

- Copyright Law
- Trademark Law
- Semiconductor Law
- Patent Law

Data protection and privacy laws aim to achieve a fair balance between the piracy rights of an individual and the interests of data controllers such as Banks, Hospitals, Electronic mail Service providers etc.

Intellectual property infringements in cyberspace may comprise of any unauthorised use or copying of trademarks, service marks protected by (Trademark Act, 1999), or original music, films, art work, software, multimedia or literary matter (protected by the Copyright Act, 1957).

The Indian Penal Code (I.P.C) (as amended by I.T Act) penalizes several cyber-crimes. These include forgery of electronic records, cyber frauds, destroying electronic evidence etc.

Digital evidence is to be collected and proven in the Court of Law as per the provisions of **the Indian Evidence Act** (as amended by the I.T. Act 2000).

Section 51: When copyright infringed- of Copyright Act

Copyright in a work shall be deemed to be infringed—

(a) when any person, without a licence granted by the owner of the copyright or the Registrar of Copyrights under this Act or in contravention of the conditions of a licence so granted or of any condition imposed by a competent authority under this Act—

> (i) does anything, the exclusive right to do which is by this Act conferred upon the owner of the copyright, or
>
> (ii) permits for profit any place to be used for the communication of the work to the public where such communication constitutes an infringement of the copyright in the work, unless he was not aware and had no reasonable ground for believing that such communication to the public would be an infringement of copyright; or

(b) when any person—

> (i) makes for sale or hire, or sells or lets for hire, or by way of trade displays or offers for sale or hire, or
>
> (ii) distributes either for the purpose of trade or to such an extent as to affect prejudicially the owner of the copyright, or
>
> (iii) by way of trade exhibits in public, or
>
> (iv) imports into India, any infringing copies of the work Provided that nothing in sub-clause
>
> (iv) shall apply to the import of one copy of any work for the private and domestic use of the importer.

Explanation. For the purposes of this section, the reproduction of a literary, dramatic, musical or artistic work in the form of a cinematograph film shall be deemed to be an "infringing copy".

Section 52 of the Copyright Act. Certain acts not to be infringement of copyright-

(1) The following acts shall not constitute an infringement of copyright, namely:

> (c) transient or incidental storage of a work or performance for the purpose of providing electronic links, access or integration, where such links, access or integration has not been expressly prohibited by the right holder, unless the person responsible is aware or has reasonable grounds for believing that

such storage is of an infringing copy:

Provided that if the person responsible for the storage of the copy has received a written complaint from the owner of copyright in the work, complaining that such transient or incidental storage is an infringement, such person responsible for the storage shall refrain from facilitating such access for a period of twenty-one days or till he receives an order from the competent court refraining from facilitating access and in case no such order is received before the expiry of such period of twenty-one days, he may continue to provide the facility of such access;

INFORMATION TECHNOLOGY ACT

In India, intermediaries are governed under the IT Act, which defines an intermediary as "any person who on behalf of another person receives, stores, or transmits that electronic record or provides any service with respect to that record".

This definition is very wide and covers a diverse set of service providers, ranging from Internet service providers, search engines, web hosting service providers, to e-commerce platforms or even social media platforms.

U.S. DIGITAL MILLENNIUM COPYRIGHT ACT (DMCA)

DMCA, Title II, the Online Copyright Infringement Liability Limitation Act ("OCILLA"), creates a safe harbour for online service providers (OSPs, including ISPs) against copyright infringement liability, provided they meet specific requirements.

OSPs must adhere to and qualify for certain prescribed safe harbour guidelines and promptly block access to alleged infringing material (or remove such material from their systems) when they receive notification of an infringement claim from a copyright holder or the copyright holder's agent.

The Act also includes a counter-notification provision that offers OSPs a safe harbour from liability to their users when users claim that the material in question is not, in fact, infringing.

Super Cassettes Industries Ltd. vs Myspace Inc. & Another

(Justice Manmohan Singh, Delhi High Court on 29 July, 2011)

The case of Super Cassettes Industries Ltd. v. Myspace Inc. although pending final judgment, is already considered a landmark example of the application of copyright law to hold an intermediary liable for infringement. In this case, the Court found Myspace guilty of primary copyright infringement for allowing the viewing and sharing of images and music over which Super Cassettes claimed ownership. Though Myspace argued that they are an intermediary within the meaning of the IT Act and are thus exempted from liability for third-party activities on the website, the court did not agree with this argument on various grounds, finding that Section 79 of the IT Act (which provides safe harbours) has to be read in conjunction with Section 81 of the IT Act which gives precedence to the Indian Copyright Act. This case is pending final determination.

COPYRIGHT PROTECTION OF COMPUTER SOFTWARE / PROGRAM

Under **the T.R.I.P.S Agreement**, computer programs now qualify for copyright protection just as any other literary work, as well as other forms of I.P. protection. Copyright, matters most in the computer software industry to off- the shelf business applications sector.

Under T.R.I.P.S, developing countries are permitted the flexibility to allow reverse engineering of software.

For the first time in India, the copyright law clearly made several provisions in this regard to protect the copyright owners: -

1. The right of a copyright holder
2. Position on rentals of software
3. The rights of the user to make backup copies
4. Section 14 of Copyright Act makes it illegal the distribution of copies of copyrighted software without paper or specific authorization.
5. The violator can be tried under both the Civil and Criminal Law
6. Heavy punishment and fines for infringement of software copyright.
7. Section 63(B)-Stipulates a minimum full term of 7 days, which can be extended up to 3 years

INTERNET PROTECTION IN INDIA

The internet challenge for the protection of internet is the protection of intellectual property. It is still unclear as to how copyright law governs or will govern these materials (literary works, pictures and other creative works) as they appear on the internet.

Section 79 of the I.T. Act 2000 provides for the liability of I.S.P's "Network Service Providers not to be liable in certain case."

Section 79 of the I.T.Act exempts I.S.P's from liability for third party information.

Indian Cyber Jurisdiction

Though it is the in nascent stage as of now, Jurisprudential development would become essential in the near future; as the internet and e-commerce shall shrink borders and merge geographical and territorial restrictions on jurisdiction. There are two dimensions to deal with.

(i) Manner in which foreign courts assume jurisdiction over the internet and relative issues

(ii) The consequences of decree passed by a foreign court.

Copyright Problems

The internet poses two basic challenges for I.P.R administrator. What to administer? and How to administer? One of the basic copyright issues in the internet is determining the border between private and public use. The Indian Copyright Act,1957 (amended in 1994, 2012) also makes a distinction between reproduction for public use and can be done only with the right holder's permission, whereas the law allows a fair dealing for the purpose of private use, research, criticism or review.

The right of reproduction presents certain fundamental problems over the internet. This is because of the basic nature of internet transmission. Reproduction takes place at every stage of transmission. Temporary copying (known as caching) is an essential part of the transmission process through internet without which messages cannot travel through the networks and reach their destinations. In the Indian Law, reproduction has to be in a material form but includes "storing of it in any medium by electronic means." Case laws need to make it amply clear about the temporary and permanent reproduction, that takes place in the internet communications.

RECOMMENDATIONS

The elaborate discussion in the foregoing chapters needs to culminate with the following recommendations: -

1. T.R.I.P.S Agreement, wherein computer programs qualify for copyright protection, needs to be adopted and implemented in letter and spirit by all the developed countries

2. Copyright, matters most in the computer software industry to off the shelf business applications sector in developing countries which presents two main problems that have to be closely monitored so that the copyright owners across the World will be protected.

> (a) Stronger protection and enforcement could mean a more limited diffusion of technologies. Eg: governments and donor organisations should review their software procurement policies.
>
> (b) National copyright laws need to be drafted appropriately.

3. Serious and sincere efforts are made for procurement of computer software. Since software license fees affect the total cost of an I.T system.

It would be sensible if the governments and donor organisations should certainly consider supporting programmes to raise awareness about low-cost options, including open-source software, in developing countries.

CONCLUSION

In view of the discussions herein the following conclusions are made: -

1. The boundaryless nature of internet calls for a more encouraging relationships in other jurisdictions and close cooperation with the international organisations
2. There is an immense need for the society to be educated about the necessity of copyright protection in all fronts to prevent any unauthorized use and pilferage of the system.
3. The copyright law is the most potent instrument presently available for tackling I.P.R issues on the internet.
4. The analysis of copyright in cyberspace reveals a mixed result of new opportunities and threats. Such threats often outweigh the opportunities offered by the cyberspace and necessity arises for increasing regulations of cyberspace to protect copyrights.
5. Lack of internationally agreed principles relating to copyrights in cyberspace gives ample room for divergent domestic standards.
6. The following exceptions and limitations to the rights need to be reassessed

    (i) Access controls ability to engage in fair use

    (ii) Circumvention of access controls affect, value and works protected by copyright.

REFERENCE

1. Gautam, Ritu, Cybercrimes and International legal regime, Available at: https://shodhganga.inflibnet.ac.in/bitstream/10603/250817/10/10_chapter-iv%20%20cybercrime%20issues%20and%20international%20legal%20regime.pdf
2. Gautam, R., Kulshrestha, P., & Goswami, M. A. K. (2021). Mediation And Family Dispute Resolution Mechanism: A Case Study On Clinical Legal Education. Elementary Education Online, 20(3), 2490-2490.
3. Gautam, R., "Proliferation of Cyber Crime and Indian legal system with special reference to Gwalior Division" Available at: https://shodhganga.inflibnet.ac.in/handle/10603/250817 Retrieved on: 22/07/2021
4. Pandey, N., Gautam, R., "property right of women in patriarchal indian society: a comprehensive study on legal narrative" Available at: https://www.researchgate.net/publication/361733554_PROPERTY_RIGHT_OF_WOMEN_IN_PATRIARCHAL_INDIAN_SOCIETY_A_COMPREHENSIVE_STUDY_ON_LEGAL_NARRATIVE_PROPERTY_RIGHT_OF_WOMEN_IN_PATRIARCHAL_INDIAN_SOCIETY_A_COMPREHENSIVE_STUDY_ON_LEGAL_NARRATIVE
5. Gautam, R., Medical health condition of prisoners and discrepancy in facilities among the states of Uttar Pradesh, Haryana and Delhi, International Journal of Health Sciences Follow journal, DOI:

10.53730/ijhs.v6nS6.12256

6. Gautam, R., Kanpur Philosophers ISSN 2348-8301 Vol IX, Issue V (IV), 2022151EFFICACY OF PROCEEDINGS OF CONCILIATION AND SETTLEMENT OF ANINDUSTRIAL DISPUTE UNDER INDUSTRIAL DISPUTES ACT, 1947, A CRITICAL Analysis. Available from: https://www.researchgate.net/publication/361733673_Kanpur_Philosophers_ISSN [accessed Sep 11 2022].
7. Gautam, Ritu, Cyber crime in India, Availablr at: http://hdl.handle.net/10603/250817
8. http://www.oznetlaw.net/fact sheets/database protection
9. http://www.legalservicesindia.com/article/2394/Challenges-of-Copy-Right-And-Cyber-Space.html#:~:text=Copyright%20threats%20are%20not%20limited,I.P.R)%20threats%20in%20the%20internet.
10. Copyright act 1957
11. Sec.43 of I.T. Act, 2000
12. http://www.linfo.org/database.html (accessed on 23/10/2008)
13. Jain, Pankaj & Rai, Pandey Sangeet CPT Laws, 2005 at Page No: 45
14. Declaration of W.I.P.O (Stockholm, July 14th, 1967)
15. http://www.bitlaw.com/source/17usc/102.html, dated 08-08-2006
16. James M.Jordan III Copyright in an Electronic Age
17. Gimber (1998), IPL 50 Stan L. Rev 1671
18. http://www.copyright.gov/legislation/hr2281.pdf,dated 10-08-2006
19. Sec.1201 (a) (1) D.M.C.A 1998
20. Sec.1201 (a) (2) D.M.C.A 1998
21. Saha.Subhasis & Kesari Sourav, JIPR Vol.13, Jan 2008 at Page No: 35
22. Law relating to intellectual property by Dr. B.L.Wadehra

24

THE NUANCED FORMS OF SEXUAL VIOLENCE IN THE ONLINE ENVIRONMENT

KEYWORDS

CRIMINAL LAW, SEXUAL VIOLENCE, DIGITAL FORM, ONLINE CONTENT, LEGISLATIVE MACHINERY

CHAPTER TWENTY FOUR

THE NUANCED FORMS OF SEXUAL VIOLENCE IN THE ONLINE ENVIRONMENT

AUTHOR

SANJUM BEDI, ASSISTANT PROFESSOR, AMITY LAW SCHOOL, AMITY UNIVERSITY, HARYANA, INDIA

ABSTRACT

With trending globalisation, massive challenges are being faced by International and National Criminal Law . It is not always the facilitated acts of gender violence but even the threats of such acts which result in psychological, physical and sexual harm to the women , children and their dignity. There is no universally applicable criminal law regime regulating online violence against women. Increase in online sexual offences grows an appetite for addressing online content through legal regulation. The national legislative developments are not potentially designed to address the typical digital sexual crimes and fallacies. Therefore, it is reflected that that there is very little shift in attitudes towards legal regulation of digital platforms which have become the biggest resource of sexual offences against women and children. The regulation of the online content becomes tough mainly due to the shield provisions maintained to ensure that platform operators are not responsible for the content that is posted and shared on their platforms. The magnitude of various forms of online sexual ferocity is mostly paired with the facelessness of the perpetrators. This is the reason of lack of appropriate and effective reporting mechanisms which poses

a barricade to the effective processing of such cases. The existing criminal law provisions incline towards focussing on concepts such as 'proximity' or 'hearing' which prove redundant in the context of acts taking place in the online sphere, mainly on social media. Image-based sexual abuse and voyeurism, have been the subject of a speedy law reform in many countries across the world but there are significant deficiencies in the way that criminal law conceptualizes the digital form of sexual violence.

"Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say."

-Edward Snowden

SUBJECT MATTER OF THE STUDY

With trending globalization, massive challenges are being faced by International and National Criminal Law.[1] It is not always the facilitated acts of gender violence but even the threats of such acts which result in psychological, physical, and sexual harm to the women, children, and their dignity. There is no universally applicable criminal law regime regulating online violence against women.

An increase in online sexual offenses grows an appetite for addressing online content through legal regulation.[2] The national legislative developments are not potentially designed to address the typical digital sexual crimes and fallacies. Therefore, it is reflected that there is very little shift in attitudes towards legal regulation of digital platforms which have become the biggest resource of sexual offenses against women and children.[3] The regulation of the online content becomes tough mainly due to the shield provisions maintained to ensure that platform operators are not responsible for the content that is posted and shared on their platforms. The magnitude of various forms of online sexual ferocity is mostly paired with the facelessness of the perpetrators. This is the reason for the lack of appropriate and effective reporting mechanisms which poses a barricade to the effective processing of such cases.[4] The existing criminal law provisions incline towards focussing on concepts such as 'Proximity' or 'Hearing' which prove redundant in the context of acts taking place in the online sphere, mainly on social media. Image-based sexual abuse and voyeurism, have been the subject of speedy law reform in many countries across the world but there are significant deficiencies in the way that criminal law conceptualizes the digital form of sexual violence.[5]

REVIEW OF RELATED LITERATURE

[1] Shirin Ahmadi Dastjerdi, et al., *The Effects Of The Globalisation On The National Criminal Law Systems,* 2614 LIBRARY PHILOSOPHY AND PRACTICE 2, 2-3 (2018)

[2] Y. ANDREW CRANE, DIRK MATTEN, ABAGAIL MCWILLIAMS, JEREMY MOON, & DONALD S. SIEGEL, THE OXFORD HANDBOOK OF CORPORATE SOCIAL RESPONSIBILITY 5-7 (Oxford University Press 1st Edition 2009)

[3] Bhartiya Shree Shakti, " A Comparative Study Of Impact Of New Laws, Crime Rate and Reporting Rate, Change In Awareness Level" , Tackling Violence Against Women: A Study Of State Intervention Measures" March, 2017, 126

[4] Nicola Henry, et al. Sexual Violence in the Digital Age,25(4) SAGE JOURNALS (2016)

[5] Alexy, E. M., Burgess, A. W., Baker,&T., Smoyak, 5 Perceptions of cyberstalking among college students SA, 279, 279-289 (2005)

The literature available and information from the internet have been studied in the proposed study. Here in after follows an attempt to review the relevant literature:

Majid Yar in his book *Cyber Crime and Society* delivers a strong, organized, and serious overview to present discussions and debates about cybercrime. It narrates the phenomenon in the extensive frameworks of the social, dogmatic, educational, and commercial change. It draws upon perspectives covering law, sociology, politics, criminology, and cultural studies to scrutinize the whole series of cybercrime concerns and disputes.[6]

Chandrima Khare in his blog on *Punishing Cyber Stalking and Online Harassment states that* India has not only shot one of the top levels for having the utmost number of internet consumers, but we also top the figures of global sexual harassment. The harassment faced by women online reflects the image of harassment faced by them in the physical world. A survey found that 50% of women in major cities of India have confronted online sexual harassment. What is striking in this is that instances of cyberstalking against women is on an extreme upwelling.[7]

Ananath Prabhu G and Vivek Shetty in their E-book *Cyber Safe Girl* through their pictorial demonstration explain that Cyber Crime is a global phenomenon that obstructs the privacy and security of a person online. Women are often the easy targets. Some people are on the lookout for personal information, like passwords, bank details, etc. Apart from that women are often exploited, stalked, harassed, and threatened in the virtual world.[8]

M. Zona, R. Palarea and J. Lane in their book *The Psychology of Stalking: Clinical and Forensic Perspectives* have made an appreciable effort to explain Cyberstalking, characterized by the stalker's persistent search of the victim online and are likely to include or evolve into some form of an offline attack as well. Many a time, the accused are unknown to their victim. However, sexual exploitation is often driven by revenge, hate, anger, jealousy, obsession, and mental illness. Cyber harassers are often driven by extreme sexual desire which leads them to frighten or embarrass the victim.

STATEMENT OF PROBLEM

It is pertinent to note that before one opts to take a legal course of action being a victim of any form of cybercrime, the most difficult thing is to trace evidence in the virtual world.[9] Though a lot of steps have been taken to curb the menace of online sexual exploitation but what is visible is the spike in such cases. The Companies were unable to frame uniform and global guidelines to device a decent 'Work From Home' environment according to the instructions by the National Commission for Women.[10] This includes devising of proper dress code, setting fixed time slots for video calls for the women especially, maintaining a proper council or commit-

[6] YAR MAJID, CYBER CRIME AND SOCIETY 100 (2006)

[7] Khare Chandrima, *Punishing Cyber Stalking and Online Harassment, IPLEADERS (Jan 29,2022, 10:04 AM)., https://blog.ipleaders.in/cyber-stalking/.*

[8] G Prabhu Ananath & Shetty Vivek, *Cyber Safe Girl*, (February 4,2022.11:00AM (2019) https://police.py.gov.in/Cyber%20Awareness%20-%20Cyber%20Safe%20Girl%20v2.0.pdf

[9] Choi KS, Lee H, Park G &Han C.,*Virtual Reality Program in Cybercrime Investigation: A Pilot Study Examining Search and Seizure of Digital Evidence Practice*, CYBERPSYCHOL BEHAV SOC NETW., 43, 43-45(2022).

[10] National Commission for Women, *India on Lockdown: Covid 19 and Women*, RASHTRA MAHILA 2020 at 01.

tee for addressing matters of online sexual exploitation at the workplace specifically during the Pandemic. [11] It has been seen that most of the websites provide a platform for reporting against sexual harassment as it is mandatory to do so for the organizations under the IT Rules, 2011, to take action within 36 hours of reporting to prohibit the foul content from spreading.[12] The casual culture is that women stop themselves to report such incidences to secure their reputation. They have inhibitions to approach the cyber cells to initiate investigation against cybercrime causing sexual harassment such as Stalking. Provisions like 354-A, 354 D, or 509 of Indian Penal Code, 1860[13] prescribe punishment for a perpetrator who sexually harasses a woman by stalking her on the internet and through his words or acts or gestures intends to insult the modesty of a woman.[14] During the pandemic, when a nationwide lockdown was announced, the problems of cyber-bullying, getting unwarranted video call requests at odd hours and online stalking had increased manifold and as usual, this time also the issue of increase in sexual harassment has been overlooked as ever before.

It should be noted that PoSH Act, 2013 makes it mandatory for the organizations to frame policies against sexual harassment which enables women to report and that too anonymously.[15] However, in the absence of the PoSH committee, women can seek the option of the Information Technology Act, 2000 which protects such harassment. [16] Section 67 of the IT Act prescribes punitive measures for publishing and/or transmitting obscene content on an electronic platform.[17] Section 67A stipulates punishment for publishing or transmitting material containing any sexually explicit act, in an electronic form.[18]

HYPOTHESIS

Glaring inadequacies can be observed in the existing laws on combating online sexual abuse against women and children. Another cause of inefficiency in tackling online sexual abuse, especially through the online platform is poor enforcement of existing laws.[19] The gross deficiency of national initiatives fail to strike at preventing national policies and/or initiatives aimed at preventing and combating online sex abuse of women are grossly deficient in India and hence, the mechanism set up in India for combating online sexual abuse and aftercare services are insufficient in a way that most of the concerned legal provisions come to action when an online sexual offense has already taken place after which tracing the wrongdoer becomes difficult because of the extra immunity provided to the online intermediaries in such cases.

[11] Ahuja K. Kanika & Padhy Priyanka, *The Cyber Avatar of Sexual Harassment at the Workplace: Media Analysis of Reports During COVID-19,* JOURNAL OF PSYCHOSEXUAL HEALTH*,* 322, 322-323 (2021)

[12] Joseph Vinod, Basu Protiti &Bhargawa Ashwarya ,A Review Of The Information Technology Rules, 2011,Reasonable Security Practices And Procedures And Sensitive Personal Data Or Info, MONDAQ (December 30, 10:00A.M.2020) http://meity.gov.in/content/preliminary

[13] Indian Penal Code, s. 354-A, s. 354 D, s. 509

[14] MISRA,S.N., INDIAN PENAL CODE*,* 678-679 (2014,Central Law Publications, Allahbad)

[15] Salient Features of the Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013, & the Rules made thereunder

[16] GUPTA RIRU, SEXUAL HARASSMENT AT WORKPLACE- A DETAILED ANALYSIS OF THE SEXUAL HARASSMENT OF WOMEN AT THE WORKPLACE (PREVENTION, PROHI BITION, REDRESSAL) ACT, 25, 2013, 151-152 (Ist ed., 2013)

[17] Information Technology Act of 2000 s. 67

[18] Information Technology Act of 2000 s.67A

[19] Laer, van Tom, *'The Means to Justify the End: Combating Cyber Harassment in Social Media'* (2014) Bus Ethics at 85, 85-98 (2014)

SEXUAL VIOLENCE AND CYBERSPACE

Voyeurism has been discussed under section 354C of IPC. This section explains that distributing images of a woman engaged in a private act is prohibited and is punishable. Even if a woman had given consent to take her pictures but did not allow them to be shared then sharing her pictures is a crime. Voyeurism is also a crime under the IT Act irrespective of gender. Section 67A of the IT Act states that if material which is published online is sexually explicit, the person can be imprisoned for 5 years and be liable to pay a fine of up to ten lakhs. Sec72 of the IT Act is employed when it comes to Online Stalking. [20]Section 72 describes the penalty for breach of confidentiality or privacy.[21] Section 354D of IPC does not explicitly cover cyber-stalking. The judicial trend shows that it is quite easy to get bail in such cases.[22]

It is pragmatic that U.K and U.S. have better legal arrangements to deal with sexual offenses conducted through digital mode. It was as early as 1999 when the U.K. charged and convicted someone for Cyber Stalking. In 2003, the UK Communications Act was introduced which precisely covers the inappropriate use of public electronic communications networks. Similarly, in the U.S the law that deals with Cyber Staking is the Violence Against Women Act. The US. Cyber Stalking has been firmly recognized as a form of violence against women through this Act.[23]

Commercial sex is to a large extent organized by the mode of the internet nowadays as the internet has become the easiest vehicle for sharing information about prostitution. The comparative anonymity of internet-based communication is a benefit for the service providers and the illegal buyers. This raises grave concern for the health industry as this kind of illegitimate business is the most common source of spreading sexually transmitted infections. However, operating a website for practicing prostitution amounts to an offense under the Prevention of Immoral Traffic Act, 1956 and is punishable but the most important challenge is that such criminals have no (digital) face which is a lacuna in the IT Act, 2000.[24]

The right to privacy and the right to freedom of speech and expression are rights that are the backbone of one's right to personal liberty. A woman has the right to dignity along with the right to life just as a man has.[25] However, these are not absolute rights. No one can violate a woman's dignity by using his right to personal liberty and freedom of speech and expression. With technological advancement, it has now become quite easy to trick a woman and gain wrongfully from her because the ways of protecting a woman are not changing whereas the forms of exploiting her are changing frequently.[26]

ROLE OF JUDICIARY

[20] Information Technology Act of 2000, s.72

[21] *Ibid.*

[22] Indian Penal Code of 1860, s 354D

[23] D. Lipton, Jacqueline,*Combating Cyber Victimization* BTLJ 1104,1116-1126 (2011)

[24] Information Technology Act of 2000, Overview

[25] INDIA CONST., art. 21

[26] *Aspects of Constitution of India, Fundamental Rights 58,* (Jan. 29, 2022, 12:00PM) https://nios.ac.in/media/documents/srsec317newE/317EL6.pdf

In *Majeesh K Mathew v. the State of Kerala*[27], the Kerala HC stated that it cannot be denied that making sexually explicit comments on social media against a woman amounts to online sexual harassment. This case was raised a thought-provoking issue — as to what constitutes online sexual harassment. The case also went in the direction of recognizing whether mere comments on a person's Facebook pictures could be treated as sexual harassment as the accused had posted certain pictures of the complainant and her spouse

on Facebook with remarks containing sexually explicit content. After going through the Facebook posts, the court found that the posts imply licentious sexual behavior. The accused's abusive behavior was a form of cyberbullying, cyber misogyny, and cyber sexism according to the court.[28]

In *Shreya Singhal v. Union of India*,[29] where the police arrested two women who posted allegedly offensive and objectionable comments on Facebook about the propriety of shutting down the city of Mumbai after the death of a political leader. The Supreme Court, based on the foregoing reasons, invalidated Section 66A of ITA.[30] It was considered to violate the right to freedom of expression guaranteed under **Article 19(1)(a)** of the Constitution of India.[31] Under section **66A of the IT Act**, a person could be charged for using the online mode for sending texts which were "grossly offensive" or of a "menacing character".[32] The Court strongly mentioned that the government is unsuccessful in showing that the law intends and anticipates to prevent communications that incite the commission of an offense because "the mere causing of annoyance, inconvenience, danger, etc., or being grossly offensive or having a menacing character are not offenses under the Penal Code at all."[33]

The Supreme Court of India in its landmark judgment of *Vishaka v. the State of Rajasthan*[34] laid down important guidelines making it mandatory for every employer to provide a redressal mechanism against grievances concerning workplace sexual harassment which are being strictly adhered to by the employers of every organization until the enactment of legislation. This case is the foundation of the law against sexual harassment of women at the workplace in India.[35] Also in *Medha Kotwal Lele & Ors. v. Union of India & Ors.*[36] the Supreme Court observed that *the implementation of the Vishaka Guidelines should be practiced in substance and spirit. It is a possible way to create a safe and secure environment for women in the workplace.*[37] *The women must be enabled to work with dignity, decency, and due respect.* In the case of *Sanjeev Mishra vs. Bank of Baroda*[38], the Rajasthan High Court stands out to be the most rational judgment in contemporary times as it widened the scope of the term 'workplace harassment' to include online harassment. This judgment is extremely supportive in the contemporary digital world as there is a global shift to the 'work from home' and women are finding themselves vulnerable to online sexual harassment. The first reported case of Cyber Stalking in India was the case of Manish Kathuria who stalked a woman named Ritu Kohli on a chat website. Manish abused her and put her phone number in the public domain. He

[27] *Majeesh K Mathew v. State of Kerala (2018)KHC 583 (India)*
[28] *Ibid.*
[29] *Shreya Singhal v. Union of India (1962) SCR 866 (India)*
[30] *Ibid.*
[31] INDIA CONST.art.19(1)(a)
[32] Information Technology Act of 2000,s. 66A
[33] Supra note 30 at 7
[34] Vishaka v. State of Rajasthan ,AIR (1997) SC 3011(India)
[35] *Ibid.*
[36] **Medha Kotwal Lele & Ors. v. Union of India & Ors. (2012),INSC 643(India)**
[37] *Ibid.*
[38] *Sanjeev Mishra vs. Bank of Baroda, (2021)SB Civil Writ Petition No. 150 (India)*

also used Kohli's identity to chat with various people. She started receiving obscene phone calls after which she reported the issue to the police. Kathuria was arrested under the charge of 509 IPC after police could trace the IP addresses.[39] This jolted the lawmakers and they woke up to the need for legislation to address Cyber Stalking which led to the introduction of Section 66-A in the IT Act, 2000.[40]

The trauma that a woman faces on being insulted sexually publicly through the digital mode can be realized by learning Vinu Priya's case who killed herself after facing backlash when her obscene pictures were posted on Facebook leaving her entire family traumatized. Instead of investigating into the matter, the police nagged Vinu Priya by assuming that she must have herself carelessly sent her obscene pictures to someone. This incident clearly shows that it is very important that a fair investigation in a proactive manner should take place without delay in such cases and the victim should not be looked down upon. [41]

Sharmistha Mukherjee, daughter of former President Pranab Mukherjee was also harassed by a man who blatantly posted sexually explicit messages on her Facebook Page. Mukherjee took the right step by sharing the screenshots of the messages sent to her and decided to speak up against online harassment but every woman does not have such support and confidence.[42]

FINDINGS

Online harassment and violence towards women reflect the stereotypical and detrimental attitudes towards women. Online sexual exploitation has become a widespread problem with the advance of technology. Online gender harassment is one of the consequences of a predominantly patriarchal society.[43] This shows the inadequacies of the current legal system to handle such cases, and the opportunities for curbing it from a policy perspective. Focussing only on data theft and fraud, rather than individual cases of harassment and violence is visible as lacunas in the working of the administration of the country. Jurisdictional boundaries and a deficiency of understanding of new digital mediums have been cited as reoccurring problems for police investigations and prosecution of perpetrators. It is for these reasons that focus must be turned towards police and the personnel should be sensitized towards this problem to enable them to see what obstacles currently stand in their way, and what can be improved. Principles of Natural Justice and Rule of Law should be imbibed while dealing with issues related to women and children because any delay in the investigation may give us more Vinu Priyas which would be unbearable.[44]

[39] Manish Kathuria v. Ritu Kohli, (2014)C.C. No. 14616 (India)

[40] Information Technology Act of 2000, s.66-A

[41] Kumaran Senthil, *Cyber Crime Cop Seeks Bribe From Bereaved Family, Suspended,* THE TIMES OF INDIA (20th Nov, 2021. 12:00PM), https://timesofindia.indiatimes.com/city/kochi/cyber-crime-cop-seeks-bribe-from-bereaved-family-suspended/articleshow/52973677.cms

[42] Mann Rashmi, President Mukherjee's Daughter Faces Online Harassment, Shames Man on Facebook, NDTV (December 5th, 2020, 1:00PM)https://www.ndtv.com/india-news/president-mukherjees-daughter-faces-harassment-puts-up-texts-on-facebook-1443834

[43] HOLLAND J. MISOGYNY: THE WORLD'S OLDEST PREJUDICE 25-30 (Ist ed. Caroll & Graf 2006)

[44] Nirola Basanta, *Patriarchy And The Status of Women In The Society*, YKA, (20 January 2022, 3:00PM) https://www.youthkiawaaz.com/2017/12/role-of-patriarchy-and-status-of-women-in-indian-society/

EXAMINATION OF HYPOTHESIS

To better provide equal and comprehensive protection to all citizens, states should consider revising their current laws on online sexual harassment to better encompass the unique aspects of Internet communication.[45]

CONCLUSION AND SUGGESTIONS

Crime against women is not a new thing. With modernization and technological advancements, anonymity can be easily maintained, and therefore, more crimes over the internet take place because of this reason. It is hard to expect and to accept that women will ever get equal treatment in this patriarchal society but what can be prayed for is proper implementation of existing laws and modifications in legal norms wherever required to create a strong legal framework. Women are often considered soft targets because the moment a woman faces sexual bullying, her character is put under a magnifying glass.[46] This attitude is hurtful and against the Rule of Law.[47] The administration of the country should take the responsibility that women are not backlashed and the police should not further suffocate the women by assuming facts that are most convenient for them to escape from carrying on the investigation. One needs to be the change that one wants to see. The women should understand that reporting such cases is vital. A single unreported case feeds such culprits with more confidence.[48] To keep up the spirit of Ubi Jus Ibi Remedium we should note what Gandhiji once said- "when the woman walks freely in the night without any fear then only it is considered as freedom." The sad reality is that this could not be possible for ages even after independence. Women have always suffered either in the name of the Sati System or the Devdasi System in earlier times. Any modern technology hits strongly on the existence of women and then proceeds to claim to do good to society. PNDT Act is a perfect example that could be seen that how humans have the natural tendency to misuse science for sex determination.[49] Women have faced deprivation for ages, it may be deprivation of food, education, or equality but now she has learned to stand for herself and seems to be no longer in a mood to suffer the deprivation of 'self-respect' and 'dignity' anymore.[50]

The government should take effective enforcement measures concerning the issue of Online Sexual Harassment. Women should be empowered by educating them. Women should get enough support from the State so that there should be no inhibition in reporting such cases.

[45] Joseph Vinod and Jain Mitali, *Anti- Cyber Bullying Laws in India- An Analysis*, MONDAQ (23rd January, 4:00P.M. https://www.mondaq.com/india/crime/989624/anti-cyber-bullying-laws-in-india--an-analysis .

[46] Keyal Nikunj, *Sexual Harassment of Women at Workplace,* (20th January, 2022, 9;00A.M. http://www.legalservicesindia.com/article/2114/Sexual-Harassment-of-Women-at-Workplace.html

[47] Hon. Maite D. Oronoz Rodriguez, *Gender Equality and the Rule of Law,* 95 NYULR 1600,1600-16003 (2020)

[48] ILO, General Survey on the fundamental Conventions concerning rights at work in light of the ILO Declaration on Social Justice for a Fair Globalization, Report III (Part 1B), 101st Session of the International Labour Confernece, Geneva, 2012, page 330.

[49] Bhaktwani Anita, *The PC-PNDT Act In A Nutshell*, Indian J Radiol Imaging. 133, 133-134(2012).

[50] AGGARWAL VIR BALA, STATUS OF WOMEN IN MODERN INDIA, 10-15 (2010) .

The police should be proactive and vigilant to deal with the cases of Online Sexual Harassment of women.[51] Awareness should be raised on social media platforms. Online safety guidelines should be followed strictly.

[51] Schuller, R.A., Stewart, A., *Police Responses to Sexual Assault Complaints: The Role of Perpetrator/Complainant Intoxication*". Law Hum Behav 535, 535-536(2000)

25

AN OVERVIEW OF CYBER PORNOGRAPHY IN INDIA

KEYWORDS

CYBERCRIME, CYBER PORNOGRAPHY, IMPACT OF CYBER PORNOGRAPHY, LAWS DEALING WITH CYBER PORNOGRAPHY, POCSO

CHAPTER TWENTY FIVE

AN OVERVIEW OF CYBER PORNOGRAPHY IN INDIA

AUTHORS

SAQUIB AHMED, RESEARCH SCHOLAR, SCHOOL OF LAW, SHARDA UNIVERSITY, INDIA

DR. RISHIKESH FAUJDAR, ASSISTANT PROFESSOR, SCHOOL OF LAW, SHARDA UNIVERSITY, GREATER NOIDA, UTTAR PRADESH, INDIA

ABSTRACT

This paper talks about the meaning and concept of cyber pornography. This paper draws light on the impact of cyber pornography and the emerging trend of cyber pornography. At the same time this paper also focusses on the current position of Indian law dealing with this cyber pornography. This study will also bring to light the new phase of cyber pornography. This paper also explains the legal position dealing with these criminal acts with the help of decided cases. Since we are living in technological age and there is always a risk of becoming target of these crimes, this paper provides better understanding of this new branch of cybercrimes and law dealing with these.

INTRODUCTION

Before understanding the concept of cyber pornography, it is extremely crucial to understand that what pornography is all about. The term pornography is derived from the Greek word “Porne graphos”. These two different Greek words has different meaning. The first word that is “prone” which means prostitute and the second word “Graphos” which stands for “writing about or description of. Pornography-”porn” or “porno” for short-is material that depicts nudity or sexual acts for the purpose of sexual stimulation. However, the presence of nudity or sexual acts in piece of media does not necessarily make that media pornographic if the purpose of that media form is something other than sexual stimulation. Pornography can take the form of photographs, videos, written material, audio recordings, or animation, among other media formats.

Even though of concept of pornography differs a bit depending upon the materials of pornography but however in legal domain pornography is defined as “obscenity”. Generally, pornography consists of obscene video, pictures, sexual clips etc which is of indecent nature.

The Oxford Dictionary defines Pornography as “printed or visual material containing explicit description or display of sexual organs or activity intended to stimulate sexual excitement”. Further, the Black’s law dictionary defines Pornography as “Lewd and lascivious materials depicting erotic images, designed to arouse sexual desire”

Earlier pornography was a narrow concept but however with the evolution of the interne and the high-speed data, pornography got widened in its scope. Since a lot of ingredients started appearing under the pornography, so the pornography got categorized under two head that is hard core pornography and soft-core pornography. There is only one major difference that existed between these two types of pornography is that hardcore pornography shows about penetration while the softcore pornography did not show any penetration.

CONCEPT OF CYBER PORNOGRAPHY

In the present scenario of online dependency, vast amount of the information is available online and hence prone to cyber threats. The widespread use of the internet facilities which have brought challenges related to cybercrime in the process of development of information and communication technology. The evolution of cyberspace has transformed the traditional pornographic content into digital pornographic content which assists the paedophiles in wide distribution, circulation of pornography materials. With the advent of science and technology, we all have witnessed the multiplication of crimes in the world. With other crimes, pornography has also embedded its roots in the society. Therefore, what was initially created for titillation of aristocrats in the form of statutes or monuments in the caves, with the help of technology, is available in high-definition video quality in our homes. Internet provides easy access to all kinds of pornography. Nowadays, you don’t even need to cross the street to get access to it. Unlock your smart phone, search for it and you are watching porn many a times without even paying for it. Pornography poses a serious challenge to the world at large.

Cyber pornography implies a demonstration by utilizing cyberspace to make, show, appropriate, import, or distributes indecent materials, particularly materials identified with youngsters who are occupied with sexual demonstrations with grown-ups. Pornography is a criminal offense which has been considered as one of the bad showing making hurt individuals. There are particular objections which exhibit different revolting material as pictures and short stimulated movies, to sound records and stories, customers use the web to make sex, sexual life, and sexual demonstrations and to coordinate sexual activities from PC screen. Web as a mode includes tremendous information and data for the individual and because of these wrongdoings identified with cyber indecency isn't inaccessible to it. Simple openness has made it more helpful for people to approach web without any problem.

In Regina v. Hicklin the main trial of indecency was set down as the inclination to debase and ruin those whose personalities are available to such indecent impacts and into whose hands a distribution of this sort may fall. Cyber pornography is perceived under .xxx' space by ICANN (Internet Cooperation for Assigned Names and Numbers) which is supported by Uniform Domain Dispute Resolution Policy, for settling debates with respect to Section names. The development of cyberspace has changed the conventional explicit substance into advanced obscene substance which helps the paedophiles in wide conveyance, flow of pornography materials.

Cyber pornography entails all forms of circulation, production and designing of explicit pornographic content, in the cyber realm. Easy accessibility and too many options have resulted in individuals perceiving pornographic content as something regular and in proximity to reality. The access has gone a bit too far, now that individuals can even upload content they wish to. Content that is not filtered, censored or approved in any way. In general terms these two terms which is "obscenity" and "pornography" are used interchangeably without any difference but however there exists some difference between them. The major difference is in their scope. The term "obscenity" has wider scope as compared to the term "pornography" because obscenity takes into consideration all the materials which are offensive, immoral and against the sentiments of the masses whereas pornography only takes into consideration sexually engaging materials. So, it could be said that pornography is a subset of obscenity.

SMART PHONES AND CHEAP DATA: CYBER PORNOGRAPHY EXPLOSION

"Anyone can access anything at any time at any place."

India has reported 95% spike in traffic to adult sites during the 3-week, first lockdown. As the Internet, particularly mobile broadband, becomes more accessible and affordable. Smart phones and cheap data availability intensify the pandemic of pornography. Indians are viewing explicit material on their mobile phones more than in any other country in the world.

It becomes easier to access pornography thanks to cheap data and smartphones. Large number of minors access explicit sexual material on their smart phones whether knowingly or just by chance enters into this red zone. The ease of carrying a phone and privacy, has been the most responsible factor for its vast use, which is not so with the computer, there was still always the chance of discovery. The little friend in our pockets made it nearly impossible to get caught in the act. Most of Indians use their smart phones as alarm clock, calculation, use to see movies, web shows and all the social media platforms etc.

Access of Banned Websites

Pornographic contents on internet are found easily on millions of porn websites and surprisingly still exist despite of banning of illegal pornography and blocking of porn websites depicting child sexual abuse materials. Banned Sexually explicit materials are available due to technical miracles which need no much expertise. Easy development of websites, VPN techniques and availability of proxy servers.

Access of Banned Sites via VPN

People are running to access banned sites via Virtual Private Network (VPN). Users continue accessing these websites via a VPN. VPN encrypts the connection from your device to the server and acts as a middle person in the process. Hence, even if people are trying to access a website that is blocked in India, the VPN requests the data from another region like Singapore or the US and then transfers the content to the user. According to Google Trends, in last some days, searches for a VPN solution shoots up abruptly.

Visits to these websites increased after the ban. In huge number of people in India are finding the bypass to access the pornographic websites which are banned. These are using the -proxy networks or virtual private networks. Which not only take the viewers to banned sites and their identities and location is also hidden. By using Opera's in-built VPN feature in 41 version by which viewers can comfortably evade the web filters provided by INS. It is two-step process where user by first connecting to the computer in foreign country and then through it access the banned websites, as:

1. Download latest version of Opera Browser.
2. Install it on your computer.
3. Open the browser once it has been installed and then go to settings. Check the box that enables the VPN.

A very easy process to access banned websites despite of efforts of courts and government, all in vain. Huge traffic is reported to increase on banned as well as unbanned porn websites in lockdown period due to COVID-19.

IMPACT OF PORNOGRAPHY AND CYBER PORNOGRAPHY

The increased use of pornography in recent decades has had a seriously detrimental effect on health and well-being globally. India has seen an increase in rape cases recently. Addiction to pornography and a rise in sexual crimes against women may be related.

India stands in third position among most porn-watching countries and fourth in the highest rape crime countries. Sexual abuse affects women's physical and mental health, as well as their sexual and reproductive health, in both short and long terms. As a result, sexual harassment is regarded as a serious public health problem. Every day, approximately 93 women are raped in India. There may be a connection between pornography addiction and an increase in sexual crime against women in India, as evidenced by the rise in rape cases. There were few reviews related to Internet pornography use and sexual motivation, learning from pornography, but there was no review on addiction to pornography and sexual violence against women in India.

Aggression and Abuse

Pornography causes deep impact on the personality of the individual. Various surveys have been conducted that shows the influence of pornography on the mindset and the personality of the individual. Those people who are addicted to pornography develops a strong sexual aggression. Sometimes this aggression is so high that pulls the individual towards the commission of the offence such as rape. In many of the rape cases it was found out that accused was in the acute addiction of watching pornographic content.

The pornographic content which is present on Internet is violent in nature. A survey conducted by the Quarter magazine reveals that more than half of the video present on the Internet consists of some or the other form of the violent content. These violent content causes major harm to human personality. It increases the violent nature of human being. People who generally watch more violent pornographic content are seen less sympathetic towards crimes such as rape and molestation. These individuals are even ready to resort to violent means to get their sexual desires satisfied.

Many NGOs are deeply concerned about the presence of violence in pornographic content and its impact on human personality. Thus, they conduct a lot of survey to know that up to what extent the violent pornographic content is hampering the personality of the masses and making them more violent. A survey was conducted by the Women's Welfare NGO to know this and 100 sexually abused women taken into study. The 58% of the women responded that their abuser was an addict of the pornography. Even though this is a small survey but it is enough to reveal the genesis of pornography in the commission of heinous offences against women. Violent pornographic content is making peoples more aggressive in nature which in turn causing increase in sexual violence.

Sexual Addiction

Sexual addiction is one of the major drawbacks of watching pornography or cyber pornography. Regular watching of online pornographic content leads to the sexual addiction which in turn causes several problems. It also leads to the development of the sexual compulsive behaviour. Sexual addiction is one of the reasons behind the growing workplace harassment cases. Sexual addiction does not only give rise to legal offences but also has major drawbacks on health of the individual. A Survey conducted in America reveals that 57% of the individuals who were the regular addicts of the online pornography were fighting with stress and depression."

There are also many major drawbacks of addiction to pornography. It leads to the lower self-esteem and the degradation of moral values of the individual. People who are addicted to any kind of pornography are seen losing their self-control over small issues and it harshly impacts their work life. So, both the online and offline pornographic content are causing several kinds of problem to the person who has become addicted to it.

Less respect towards women

Pornography often portrays women as a sexual material that could be used by men anytime, they want. In pornographic videos women are majorly highlighted as compared to the men. Women are shown as a pleasure object. These thing impacts the mindset of the porn viewers and they develop an attitude of disrespect towards women. They start treating the women as a pleasure commodity rather than the symbol of dignity. This lowers the dignity and respect towards the women community.

Violence in married life

It is observed that people who are addicted to the pornography often exercise violence in their married life. Since watching porn impacts them in several ways, they develop this attitude of exercising violence against their partner. Exercising violence against partner gives rise to the matrimonial separation, divorce and legal issues. In many cases it was seen that FIR was lodged against the individuals who was found exercising violence against their partner. Violence in married life due to the huge use of internet pornography is very common. Violence in married life is causing huge impact even on the children.

Effects on the Mind, Body, and Soul

The "digital revolution" has led to great strides in productivity, communication, and other desirable ends, but pornographers also have harnessed its power for their profit. The cost has been a further weakening of the nation's citizens and families, a development that should be of grave concern to all. The social sciences demonstrate the appropriateness of this concern.

Two reports, one by the American Psychological Association on hyper-sexualized girls and the other by the National Campaign to Prevent Teen Pregnancy on the pornographic content of phone texting among teenagers, make clear that the digital revolution is being used by younger and younger children to dismantle the barriers that channel sexuality into family life.

EMERGING TREND OF CYBER CHILD PORNOGRAPHY

Today's society is increasingly aware of the issue of online child pornography. Over the past ten years, as home PC usage has increased and access to the World Wide Web has become more widespread, child pornographers have discovered a simple outlet for disseminating graphic images of child sexual assault. Additionally, police and attorneys from all over the world have discovered that finding and prosecuting online child pornographers has become a difficult task, frequently with a high failure rate of putting offenders behind bars. The techniques now used by law enforcement to stop child pornography online could be viewed as archaic and ineffective.

Researches shows that approximately ninety percent of children between age group 12 to 18 years have access to the Internet. Their tender age and curious nature push them to know more. The increased ease of access to online pornography has also contributed to the likelihood of children's accidental exposure. Now a days production houses, media groups and other groups associated with broadcasting system are producing programmes containing adult contents showing in TV shows, videos, songs, music albums, web series like Sacred Games, Rasbhari, showing soft pornography in the programmes.

All this are freely and easily available to children and teenagers who are worst affected by the pornographic contents. Once any child or more specific teenager get exposed to soft core pornography his/her sensual desires push him to search for hard core pornography. His search for more sexually explicit contents is not tricky to peruse as internet provide all type of required data on single click and especially it is not automatically recognizing the age of the users. Children once entered in this world either knowingly or unknowingly, they definitely in majority of cases go for more due to their naturally curious brains.

In present scenario, it is getting harder day by day to ensure the protection of the children from constant introduction to sexually explicit contents. And often, they exposed to pornographic material accidentally when they are online. Internet is flooded with such sexually explicit materials, either directly or in suggestive advertisements. Certain games have sexual acts as gaming levels for example stripping of girls and boys in games or participant in sexual assault. Play boy magazine launches porn gaming site to fetch the young children.

Factors Responsible for Early Exposure

The peer groups are discussing it. Children often search sexually explicit material out of curiosity about which friends are talking. And, in-pre- and early adolescence, hormonal changes generally stimulate their interest in sexual matters. They are always in search of matters that suit their youthful age.

Children may trap in web of pornography by mistakenly written word or sentences. They might click on links in phishing or spam emails, dodgy links. Porn pop-up during searching, checking emails, during online gaming and in online advertisements. First exposed to -Soft Porn on mainstream broadcasts, and later search **for** Hard Porn out of curiosity.

Emergence of Online Child Pornography Law in India

Prior to the enactment of the Information Technology (Amendment) Act, 2008 (IT Act),

there was no law specifically targeting online child pornography in India. Child pornography was regulated by obscenity laws. For example, in a 2008 case in the Delhi High Court, where a pornographic MMS of children was circulated online on a popular site, the accused was charged under Section67 of the IT Act (Publication and transmission of obscene material) and Section 292 of the Indian Penal Code (Sale of obscene material). Noting the lack of specific legislation, Murlidhar, J stated,

"India may want to develop a different legislative model to regulate the use of the internet with a view to prohibiting its use for disseminating child pornographic materials... the task deserves the utmost priority".

During this time, there was growing consensus among the international community on the need for universal criminalisation of the production and distribution of online child pornography. To this end the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography (CRC-OP) called on state parties to penalize child pornography. India signed the protocol on 15th November 2004 and ratified it on 16th August 2006.

In India, both the Expert committee as well as the Standing committee to the IT(Amendment)Bill, 2006 recommended that a specific provision be incorporated to criminalize online child pornography. Accordingly, Section 67B of the IT Act came into force on 27th October, 2009. Subsequently, the Indian government passed the Protection of Children from Sexual Offences Act, 2012 (POSCO) which also criminalises child pornography.

Criminal Liability for Online Child Pornography

The IT Act criminalizes production, publication and distribution of child pornography. Production includes creation of any "text and digital images", depicting children in indecent or sexually explicit manner and recording "abuse pertaining to a sexually explicit act". Apart from video, audio and photographs, the definition is wide enough to include the criminalisation of the comics, erotica novels or cartoons depicting children engaging in sexual activity. The Act also prohibits all forms of publication, transmission, advertisement, promotion, exchange and distribution of material "depicting children in obscene or indecent or sexually explicit manner". While consumption of adult pornography is not a crime, Section 67 B specifically criminalises seeking, downloading, browsing or storing of child pornography. All these acts are punishable with five years' imprisonment and seven years imprisonment for all subsequent offences. There is a limited exception to the offence if the material used is "in the interest of science, literature, art or learning or other objects of general concern" or is for "bonafide heritage or religious purposes".

POSCO criminalises the use of children for pornographic purposes in any form of media including through a representation of the sexual organs of a child; (b) usage of a child

engaged in real or simulated sexual acts (with or without penetration); (c) the indecent or obscene representation of a child". Contravention is punishable with imprisonment ranging from six years to life, depending on the type of offence. The Act also criminalises the storage of any pornographic material involving a child in any form, for commercial purposes. Non-commercial consumption of child pornography is thus not punishable under POSCO.

Intermediary Liability for Online Child Pornography

Pornographic content is inevitably transmitted through one or more intermediaries. If

A uploads pornographic content to a video site Y from cyber cafe Z- the pornographic content is transmitted from Z's computer to Z's ISP B to Site Y where it is stored. Due to the "strict liability" nature of offences under Section 67B, this mere act of transmission is an offence. Thus, Z, Band Y would all be held liable, even without intention. A defence available to such intermediaries, is the absence of knowledge or consent", despite "due diligence".

The due diligence defence is codified under Section 79 of the IT Act. An intermediary is not liable for an offence if it did not

1. initiate the transmission
2. select the receiver of the transmission
3. select or modify the information contained in the transmission".

Intermediaries also have to follow the Intermediaries Guidelines, which require them to publish rules which inform users not to transmit pornographic material or materials which can harm to minors".

These guidelines also mandate disabling of violative content within 36 hours of receiving information about it from any affected person. This was problematic because intermediaries were likely to disable any content upon any complaint, regardless of validity, in order to avoid the risk of non-compliance. The Supreme Court has noted this problem and "read down" the IT Act as well as intermediary guidelines. It held that intermediaries need not take-down content unless they receive, "actual knowledge that court order has been passed asking it to expeditiously remove or disable access".

Enforcement Mechanisms

Even though the National Policy for Children, 2013 mentions protection of children from pornography as one of its goals, enforcement mechanisms under the child pornography law remain weak. As per Crime in India 2015, only 94 cases were recorded under Section 94 and 95 of POSCO and only 8 cases were reported under Section 67B of the IT Act in 2015. A UNICEF report on child pornography concluded, "Legislation, mechanisms and services are in adequate to respond to these threats and have to be updated and strengthened". The Indian government has recently attempted to improve the enforcement of child pornography laws. An Advisory was circulated to all State governments in order to prevent and combat cybercrime against Children. An e-box in the women and child welfare website and a national helpline has been launched to get reports about child pornography. The government has also engaged in consultations with stakeholders to improve enforcement mechanisms and considered the creation of National Alliance against Online Child Sexual Abuse and Exploitation.

Child pornography offences are looked upon very seriously by courts. The Supreme Court has expressed concern about child pornography and has directed a ban on all websites containing child pornography. In a possible deviation from Shreya Singhal, the court has also issued notices to intermediaries to examine filtering of child pornography. This petition is currently on going in the court.

CRIMINALISATION OF CYBER PORNOGRAPHY

Under the IT Act sending or distributing of any obscene material is illicit. The Sections in the Information Technology Act, 2000 which forbids cyber pornography yet with specific exemptions for them are-Section 67 and 67A. Section 67 arrangements with distributing or communicating disgusting material in electronic structure. The Information Technology Amendment Act 2008 has likewise included kid pornography and maintenance of records by delegates. Whoever distributes or communicates any material which is indecent or claims to the lewd interest or if its belongings will in general debase and ruin the psyche of people who are probably going to peruse, see the explicit matter contained in it, will be rebuffed with detainment for a term up to three years which may reach out to five years and fine of five lakh rupees which may stretch out to ten lakh rupees or both. The term Publication incorporate any material at whatever point moved on a site, twitter or WhatsApp social affair or some other individual to individual correspondence objections or any high level doorway through which pariahs will move toward such material. The term Transmission incorporate scattering any material having profane pictures to any person through email, messages, WhatsApp or some other sort of cutting edge entryway.

Section 67-An arrangement with appropriating or sending of material containing unequivocally express demonstration in electronic edge. Section 67C power the obligation on the agents that they will secure and hold such information as may be shown for such length and in such manner as the Central Government may suggest. Rebelliousness is an offense which attracts confinement up to three years or fine,

Section 79 of IT Act sets down conditions under which ISPS or go between are not responsible from culpability for hostile agreeable transferred by an outsider. It commits the go between to work out "due perseverance", and to follow up on the data of the court or the public authority and its organizations to meet the models for resistance.

In **Avinash Bajaj v. State** was captured for an ad by a client to sell the DPS sex outrage video. The video was not transferred on the advanced entrance, in spite of that Avinash was captured under Section 67 of the Information Technology Act. It was resulting to this case that the Intermediary rules were passed in 2011 whereby an Intermediary's responsibility will be exculpated on the off chance that they practiced due steadiness to guarantee disgusting substance isn't shown on their entrance.

In **Aveek Sarkar & Another versus State of West Bengal And Anr** on 3 February, 2014, Justices K.S. Radhakrishnan and A.K. Sikri maintained and decided that if any image or article contain lascivious material which bids to lecherous interests will in general debase and ruin those liable to peruse, see or hear it, would be considered to foul.

According to the Indian Penal Code, 1860 Section 293 "whosoever offers, lets to employ, disseminates, displays or circles to any individual younger than twenty years any such vulgar article, as is alluded to in IPC Section 292, or offers of endeavors so to do, will be rebuffed with detainment for a term which may reach out to three years, and which fine which may stretch out to 2,000 rupees, and, in case of a second or resulting conviction, with detainment of one or the other depiction for a term which may reach out to seven years, and furthermore with fine which may stretch out to 5,000 rupees. It is a cognizable offense". Section 292(2) IPC "says that, a book, freebee, paper, making, drawing, painting depiction, figure or some other dissent, will be regarded to be profane if it is obscene or solicitations to the lecherous interest or if its effect, it will be repelled with confinement, for the essential model, of one or the other portrayal for a term which may contact two years, and with fine which may loosen up to 2,000 rupees, and, if there should arise an occurrence of a second or coming about conviction, with confinement of one or the other depiction for a term which may loosen up to five years, and moreover with fine which may loosen up to 5,000 rupees".

Indecent Representation of Women's Act, 1986 tries to forbid portrayal in a revolting style of ladies or any piece of their bodies given that their portrayal is impeding to profound quality.

Section 13 of the (Protection of Children from Sexual Offenses Act), 2012 characterized the offense of kid pornography and states that any individual who utilizes a youngster for sexual satisfaction on any type of media is liable of kid pornography offense. Section 14 of the (Protection of Children from Sexual Offenses Act), 2012 gives that Whoever utilizes a youngster or kids for obscene purposes will be rebuffed with detainment for a term which will not be under five years and will likewise be obligated to fine and in case of second or resulting conviction with detainment for a term which will not be under seven years and furthermore be at risk to fine.

1. Section 15 of the (Protection of Children from Sexual Offenses Act), 2012 gives that Any individual, who stores or has explicit material in any structure including a kid, however neglects to erase or annihilate or report something similar to the assigned power, as might be endorsed, with a goal to share or send youngster pornography, will be at risk to fine at least 5,000 rupees and in case of second or resulting offense, with fine which will not be under 10,000 rupees.
2. Any individual, who stores or has explicit material in any structure including a kid for sending or engendering or showing or appropriating in any way whenever aside from the motivation

behind detailing, as might be endorsed, or for use as proof in court, will be rebuffed with detainment of either portrayal which may stretch out to three years, or with fine, or with both

3. Any individual, who stores or has obscene material in any structure including a youngster for business reason will be rebuffed on the primary conviction with detainment of either depiction which will not be under three years which may reach out to five years, or with fine, or with both and in case of second or resulting conviction, with detainment of either portrayal which will not be under five years which may stretch out to seven years and will likewise be at risk to fine.

CONCLUSION

Pornography does not affect mind when actively viewed but also when mind is full of thoughts of porn even when person is not actively viewing it. It appears that the issue of sexually explicit content has grown to be more serious than anyone could have anticipated. Due to numerous factors—both personal and official—the relationship between sexual material and audience has radically changed over time. The fundamental cause of the rise in demand for pornography is addiction. Age groups and social classes are excluded in order to maintain the effectiveness of explicit content. The availability and evolution of technology have made pornographic material readily available online.

The threat posed by cyberpornography has grown due to the internet's existence. Even though there are several laws that forbid the distribution and publication of cyberpornography, viewing it is not against the law unless it is child pornography. To put it bluntly, getting access to sexual information has never been a problem; instead, it must be kept out of the hands of the incorrect people (underage individuals) who lack a mature understanding of its sexual connotations. If empathy, concepts of permission, and sensibility are not deeply ingrained in people from the very beginning, this horrifying cyberspace crisis cannot be stopped. The threat posed by cyberpornography has grown due to the Internet's existence. Although there are a number of laws that forbid the distribution and publication of cyberpornography, it is not unlawful to see it as long as it is not child pornography. Provided that the intermediaries were careful and did not aid in the cybercrime, they won't be held responsible for any illegal publications made by users.

The government's primary challenge is to properly regulate cyberpornography. Using the Internet, minors can easily access pornographic content. The state should make an effort to educate people toward social maturity; after that, the individual should be free to choose what he wants to view. This is the most effective way to combat the threat of cyberpornography.

The parents must take a significant role in regulating their children's online behaviour. They must also educate their children and act as friends for them.

REFERENCES

Statutes

- Constitution of India
- Indecent Representation of Women (Prohibition) Act, 1986
- Indian Penal Code, 1860
- Information and Technology Act, 2000
- Protection of Children from Sexual Offences Act,2012

Journals

- Jonathan Coopersmith, PORNOGRAPHY, TECHNOLOGY AND PROGRESS, 1998, International Committee for The History of Technology (ICOHTEC)

Websites

- "CYBER PORNOGRAPHY": A THREAT TO MODERN SOCIETY | (legalreadings.com)
- Cyber Pornography: All You Want to Know about and ways to Vindicate it (ipleaders.in)
- Cyber Pornography (lawyersclubindia.com)
- Cyber pornography in India and its implication on cybercafe operators - ScienceDirect

26

INTELLIGENT SYSTEM FOR DIAGNOSIS OF PULMONARY TUBERCULOSIS USING MACHINE LEARNING

KEYWORDS

ENSEMBLE LEARNING, OPTIMIZATION, STACKING, PULMONARY TUBERCULOSIS DISEASE

CHAPTER TWENTY SIX

INTELLIGENT SYSTEM FOR DIAGNOSIS OF PULMONARY

AUTHORS

SIRAJ SEBHATU, RESEARCH SCHOLAR, COMPUTER SCIENCE AND ENGINEERING DEPARTMENT, SHARDA UNIVERSITY, GREATER NOIDA, UTTAR PRADESH, INDIA

DR. POOJA, ASSISTANT PROFESSOR, SSET, SHARDA UNIVERSITY

PROF. PARMA NAND, DEAN, SSET, SHARDA UNIVERSITY

ABSTRACT

In this research, model development is carried out under supervised learning, as the system tries to correct and update itself by comparing the outcome with the target result. After all, only one model category is used, enhanced model performance through substituting the selected features with high sensitivity and low accuracyin clinical knowledge. The experimental analysis shows that the Gradient Boosting (GB) XG Boosting model achieves the best result using the original data set to predict PTB-disease. The ensemble model composed of the Adaboost, Bagging, Random Forest, GB, and Multi-Layer Perceptron models is the best to detect. The Ensemble model reaches 97.8 % accuracy, which exceeds each classification's accuracy. The model is used to help doctors analyze & evaluate medical cases to validate the diagnosis and minimize human error. It effectivelymitigates clinical diagnosis in such difficult challenges

as microscopic scanning and reduces the likelihood of misdiagnosis. The model differentiates the patient using a voting method of different machine learning classifiers to provide accurate solutions from having only one model. The novelty of this approach lies in its adaptability to the ensemble model that is continually optimizing itself based on data.

INTRODUCTION

Tuberculosis is a disease caused by mycobacterium tuberculosis that can damage respiratory organs and affect other internal parts of the body. It usually extends throughout the air and highest-burden worldwide as one of the human infectious diseases. Especially The risk of TB attack is higher for patients with the Human Immune Deficiency Virus (HIV).In India, it is also a significant health issue on Pulmonary Tuberculosis diagnosis was always a problem. Most of the detection method needs high cost and complete power devices. Depending on the diagnosis, delayed or inappropriate treatment can result in unsatisfactory results, including the exacerbation of clinical symptoms, poor quality of life, and increased disease prevalence. Still, these devices require time and hard work [1], leading to low detection rates and incorrect diagnosis, even for experienced pathologists. Some new technologies were developed, including PCR and RNA scopes, to improve effectiveness and sensitivity in diagnosing TB bacilli, but neither has been successful and widely accepted so far.[1]Moreover, the effective diagnosis of the disease is a necessary first step towards eradicating TB. In small-income countries, where the disease is predominantly present, the method of diagnosis should be fast, precise, and easy to use. The rapid request for tuberculosis infection control measures reflects new diagnostic methods [2]. Classification of health data is essential in detecting and screening any disease. It even lets doctors make decisions about their diagnostics and treatments.

We proposed an ensemble voting approach to compare the efficiency of ensemble learning classifiers on pulmonary tuberculosis physical examination, clinical and key- population factor health data. Moreover, we usedBagging, boosting, blending, and stacking. A designed model helps to detect pulmonary Tuberculosis by using thetrained model. The most important cause of failure to control tuberculosis disease global effort is delaying appropriate treatments and misdiagnosis. Due to this reason, the patient is exposed to long-term lung damage. Studies reported that a therapy delay of more than four months (12.1 weeks) would result in a larger proportion ofpatients with chronic TB, an increased mortality rate, and a higher failure in treatment. The timeframe between thepatient's initial diagnosis and first contact with a care provider was determined as the patient's delay. The delay indiagnosis was stated as the period between first medical assessment and diagnosis [3] cough, hemoptysis, night sweats, fever, and weight loss are suggestive symptoms of TB. Such signs include not only Tuberculosis but also other diseases. According to these difficult circumstances, requests to enact potential alternative approaches for PTB diagnosis are important, bringing down the cost and time resources and improving prediction accuracy. Somestudies have been done to address these problems related to the diagnosis of TB that have been implemented usingsound, images, blood miRNA profiles, and variables as input parameters. Diagnosis and treatment parameters formicroscopy and limited period for traditional cultivation approaches have already been focused on designing accelerated methods for Mycobacterium. Bovis detection of mycobacterial isolates in clinical specimens and earlyidentification [4]. The main disadvantages are difficulty, lengthy use, and the lack of suitable techniques for bovineTuberculosis (PTB). It is highly difficult to analyze and interpret the results; it is not unique responses triggered by other mycobacterial organisms.

This research aims to build a classification model for the initial screening of pulmonary Tuberculosis (PTB) disease. This model can be applied to determine whether an individual has been infected with PTB or not, based on clinical symptoms and other key factors in the population [5]. The physical examination and clinical active pulmonary tuberculosis symptoms are coughs, fever, hemoptysis, weight loss, night sweat, duration_ predominantsymptom its duration (PDSD), Visual appearance of sputum, HIV, Diabetics, etc. [6]. Key population around theindividual exposed to the number of factors like as age, gender, contact TB person, tobacco, prison inmates, miner, migrant, refugee, urban slum, Healthcare workers associated with medical expertise have been used to train the model, [7, 8] but it does have limitations such as low accuracy, long observation time, etc. Consequently, an efficient TB screening method is needed [9]. The content of the paper is structured accordingly. The first part provides a detailed description of Tuberculosis, the problem area, background, the aim of the research, and the relevance of the research findings. The second part describes previous research related to this study. The third partwill discuss the methodologies and proposed methods used to carry out this research. Eventually, the fourth part discusses the result and conclusions.

RELATED WORK

The latest improvements in ensemble methods and massive datasets have supported algorithms to perform numerous diagnostic tasks for respiratory diseases, such as PTB classification. [10]. This model significantly improved the disease's screening accuracy compared with a ruled-based method. The study used deep learning andclassic machine learning based on physical indicators of symptoms, biochemical observations to diagnose adult asthma. Their research has lung and bronchial challenge check accuracy, 60% SVM accuracy, and 65% logistic analysis accuracy [11]. Other work considered ensemble technique enhancing the integration of various classifiers, performing high accuracy on a single ensemble model and a model provide a solution to reduce the isolation of PTB patients [2]. The ensemble classifiers ' prediction accuracy was tested using Cross-Validation (10-fold), and findings were evaluated to achieve the best prediction accuracy, for instance, Bagging and AdaBoost. The resultsshow that Bagging achieves the highest accuracy with 97%, Random Forest 93%, and Adaboost 96 % [12].

Several classification methods have been discussed. The C4.5 Tree of Decision and support vector machine was not statistically significant, compared with the SVM with Naive Bayes and the K-nearest neighbour, statistically significant. Retroviral Pulmonary Tuberculosis (RPTB) and Pulmonary Tuberculosis (PTB) together with AIDS with appropriate learning classifiers [10]. Models based on ANN help to support a tuberculosis diagnosis study under limited resources. Analyzing important information from the database MLP detection performance achieved97% of sensitivity and applying cluster techniques using SOM network comparing three risk group detecting the disease the algorithm perform 89% of sensitivity [11]. According to the analysis, which applies Support Vector Machine (SVM) and decision tree (C5.0) based on a multi-objective gradient evaluation, medical test PTB can easily detect infection and achieve a more reliable diagnostic outcome[12].

On the one hand, classification of PTB based on a random forest model that performs early diagnostic optimization 81% of the area under the curve (AUC)[13] and the other study in 2017 using SVM, C5.0 shows the results of themodel perform as better accuracy of 85.54%[14]. At the same year assessment of PTB characteristics using the neural network, the model performs with the highest accuracy using the pruning method [15]. The decision tree also optimizes the time to verify results compared to the nearest k neighbours [16]. A classification model based on a single MLP with a better accuracy performance obtained a sensitivity of 83.3% and specificity of 94.3%[17].The most significant factors found by the clustering are the TB evaluation findings indicating that patients with Hemoglobin used their age, sex, smoking, and alcohol.

METHODS

Ensemble Methods for Prediction of Pulmonary Tuberculosis Diagnosis

Ensemble methods (EM) represent people's co-decision process in the treatment of hard decisions. The core idea in machine learning is to create strong predictors with weak but distinct models combined [18]. In most cases, EM's goals are to achieve more effective and robust solutions than alternative individual models to solve complexproblems [19].

Generally, the study includes three main phases: processing of specific classifiers, selection of members, and specification of the decision process. Independent errors on the models generated to integrate the group should occur to optimize ensemble performance, which does not result in approaching strategies that explore data, structural variables diversity [19]. This optimization is expected to have small clustered errors in various models,thus improving committee performance and complementing each other. Key approaches to creating diverse models include using various training sets, model hyper-parameters, and classification methods. Data interoperability is among the most efficient methods, based on most of its extensions on the well-known Random Forest, Bagging, and Boosting algorithms [18].

Bagging is roughly focused on preparing various training to design "supposed" models. A specific training set is generated from an original random sample of bootstrap (BS), i.e., a replacement sampling. A baseline classifier iscreated for each BS, and the committee's output is an average of the outputs of each model. For each BS, a differentclassifier generates a base algorithm, and the result of the committee consists of an average of all outputs of the models. In later years, several bagging combinations were advocated, most of them considering strategies to reducethe number of baseline classifiers involved in the groups by the sequential backward selection, genetic algorithms,and clustering.

Data Source and data descriptions

Further experiments have shown that an appropriate selection method is more compatible with class members andmitigates the class difference effects. Alternative decision fusion mechanisms are often discussed, such as reducingthe ensemble output variance.

In this work, standard datasets (from the Wolaita Sodo University Teaching Referral Hospital) are employed to evaluate an intelligent system for Pulmonary Tuberculosis diagnosis. In the following, the data sets are listed briefly described below in Table 1. The medical data we describe contains 3252 individual TB patient records. The whole file with many documents is stored in one file. That record is consistent with one patient's most relevantdata. Initial doctor inquiries as symptoms and necessary patient test details were major attributes. A class has 19 symptoms, such as gender, age, cough, fever, hemoptysis, weight loss, night sweat, predominant period symptom(PDSD), the visual appearance of sputum, HIV, diabetics, and other main population factors contact TB person tobacco, inmates, miners migrants, refugees, urban slums, health care workers, and also the class outcome of the attribute namely early diagnosis. Table.1 shows the names of 19 different attributes listed along with their categorical and numerical together with the data type.

Table 1. List and data types of attributes

	Name of Variables	**Data Types**
1	Age	Numerical
2	Gender	Categorical
3	Contact TB person	Categorical
4	Tobacco	Categorical
5	Prison Inmates	Categorical
6	Miner	Categorical
7	Migrant	Categorical
8	Refugee	Categorical
9	Urban Slum	Categorical
10	Healthcare Worker	Categorical
11	Cough	Categorical
12	Fever	Categorical
13	Hemoptysis	Categorical
14	Weight Loss	Categorical
15	Night Sweat	Categorical
16	Duration of symptom	Numerical
17	Sputum a. Mucopurulent	Categorical
	b. Saliva	
	c. Bloodstained	
18	Human immune Deficiency Virus (HIV)	Categorical
19	Diabetics	Categorical

Feature Selection

We recommend three methods of selection: wrapper selection procedure, filtering of features using decision trees,and removing highly correlated technical attributes. We will compare and contrast the accuracy of the classification with the features chosen using each of the techniques. Finally, we pick the most appropriate set of features [20]. Feature selection with reverse function elimination is a greedy algorithm for searching. It continues with all available features and then drops one feature at a time [21]. We use the reverse isolation of ranking attributes to make this algorithm more effective. The optimal subset function may not be special, as specific function sets mayachieve the same accuracy (e.g., two correlated features may replace each other) [21]. Backward isolation can more easily capture interacting features using backward elimination.

Missing Value Treatment Method

Treatment of missing values using the imputation technique [22, 23] is the popular missing data treatment technique in which missing values are replaced by a certain approximate value in combination with the available data set. The purpose of this technique is to use correlations to help estimate missing values, which can be contained in the valid values of the data set. In [24], investigators investigated the efficiency indicator of zero substitution and trajectories, the mean trajectory, singular decomposition value (SVD), and a weighted kNN method to replace missing values in medical datasets and stated that the kNN method is equivalent to the inferenceof missing values. The nearest neighbours, the Euclidean distance measurements, are determined by minimizing the distance function [24].

Combination of Ensemble Voting Technique

The first word used, Bagging, is slang for the bootstrapping and aggregating combination. Bootstrapping is a technique for reducing the classification variance and minimizing overfitting by re-examining training sets with the same cardinality as the entire set. The produced model should be less extreme than a single model. High variance is not good for a model, so its efficiency is sensitive to the data provided. Thus, the model can work poorly,even if more data is given. And the variance of our model may not even be reduced [18]. Suppose a set of simplelearners is generated, and not after trying to find the best single pupil. In that case, ensemble methods depend on combining these methods to achieve the best generalization results. The fundamental reasons are the statistical issue and computational issue.

Consequently, the statistical problem is generally too large to explore hypotheses for limited training data set andmany different hypotheses that give training data accuracy. Suppose the learner algorithm chooses one of the hypotheses; moreover, the importance of combining the hypotheses is reducing the wrong choice of the hypothesis[18, 19]. Additionally, Computational often conducts a certain different local search which is stuck in optimal localnumbers with many learning algorithms. It can still be very challenging to find the best hypothesis even if sufficient training data are available; using the combination could provide a better estimate of a true unknown hypothesis from a local search from several different starting points.

Designing Different Types of Bootstrap Samples

The majority of design a set of new ensembles approach, which focuses exclusively on model selection, our proposal provides for the generation of a set of various bootstrap samples, using a low-cost computational procedure. Some bootstrap samples are the fundamental concept (BSs) (βT, β > 1) applicants, selecting the T mostdifferent from the existing training dataset (ETS), where T is a user-defined parameter, and n attributes denoted by C1, C2…Cn classifier, BS-1, BS-2...BS-n bootstrap. We designed a mechanism to determine the degree of similarity of the existing training dataset (ETS) and certain bootstrap samples (BS) [18, 19].

Soft Voting

$T^1 \sum_{X=1}^{T} h^j{}_i(X)$The majority voting plurality and weighted votes for individual classifiers generating class labels can be used, while the soft vote is usually the option for individual classifiers producing class likelihood outcomes. With the soft weighted vote, with each classifier, we measure a percentage weight. For each model of record, a predicted class likelihood is obtained and increased by the weight of the classifier and is finally averaged [22, 23]. The finallabel of the class comes with the highest average likelihood from the class label. Besides, weights are difficult to find if you only offer your best estimates of which model you assume should be more or less weighted [2]. A deterministic optimization equation or neural net can be built to counteract this subjective process to determine theright weighting of each model to optimize the higher performances of ensemble model accuracy. Here the individual classifier hi outputs, a one (l)-dimensional vector (h□□ (X)……., h□□ (X)) □ for the instance X, where h□□ (X)□ [0, 1] can be regarded as a prediction of the posterior likelihood P (□□ □ X). if all the individual equivalent consideration of classifiers, the simple soft voting method generates the combined output by simply averaging all the individual outputs, and the final output for class C□ is given by Soft voting for homogenousassemblies is commonly used. The class probabilities created by different types of learners can not necessarily becompared for heterogeneous classes without careful calibration, the class probability outputs are often converted to class label outputs by setting h□□ (X to 1 if,h□□ (X) = {max□ (X)} and 0 otherwise, and the voting methods for crisplabels can be applied [18, 22].

Bagging

Bagging is a whole approach used for various training datasets to achieve different classifications, which used theexisting learning algorithm. A bootstrap technique for re-sampling the training dataset improves the difference of the training datasets [24]. This approach eliminates noisy data, outliers, variance, As Fig.1 shows. Every classifierthen receives training on a re-sample of instances, which assigns to these instances a predicted class.

The estimatesof the various classifiers (with equal weight) are then combined by majority voting. The significance of this approach to support boosts a model disease detection accuracy and consistency of a machine learning algorithm[19].

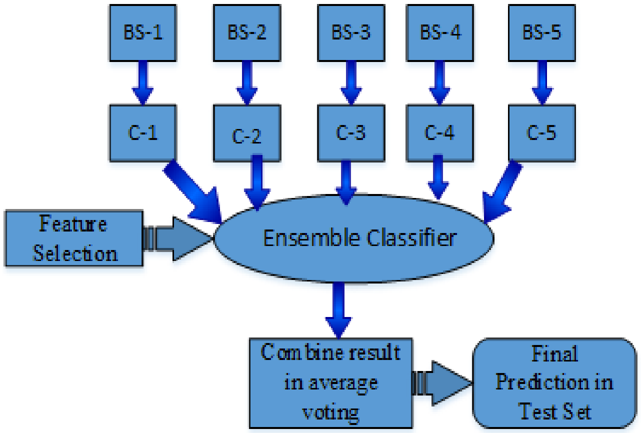


Fig.1 The ensemble model Process

The top-level model takes the low-level performance and allows the estimation of the stacking algorithm presentedin Fig. 1. The initial data is processed as input to several individual models in stacking. Then the Meta classifier estimates the input and output of the respective model, and the Meta classifiers' support using the weights of eachclassifier for prediction [18, 23]. The highest performing model results are selected, and the left the remains. Stacking combines multiple base classifiers trained by using different learning algorithms L on the existing datasetS, utilizing a Meta classifier.

```
Let D= {bs-□ , bs□ , b-□ , bs-□ , bs-□ …….bs-□ } e the
givendataset

E = {}, the set of ensemble classifiersC =
{c□ , c□ , c□ … ....c□ }, the classifiers

X = the training set, X□ D Y =
the test set, Y □ D

L = n (D)

For I = I to L do

S (i) = {Bootstrap sample I with replacement} 1 □ XE
= E U C (i)

Next I

For I = 1 to L
```

R (i) = Y classified by E (i)Next i

Result = max (R (i): i=1, 2… n)

EXPERIMENTAL ANALYSIS AND RESULT

The Ensemble Classifier Performance

A comparative study is conducted on the original dataset of various classification algorithms. Some algorithms have a strong precision, while others are weak. Multiple ensemble Classifiers are used to boost the effectiveness of the weak classifiers. This study used group algorithms such as Bagging and Stacking. The Bagging algorithm Table.2 (a & b) sows execute an ensemble with the Bagging Random Forest Classifier, Bagging ExtraTrees Classifier, Bagging KNeighbors Classifier, Bagging SVC, Bagging Ridge Classifier algorithms.

Table.2 (a). Improvement in Boosting Accuracy

Accuracy	**Standard**	**Classifier**
Mean of: 0.968	(+/-) 0.0012	Bagging Random Forest Classifier
Mean of : 0.896	(+/-) 0.002	Bagging Extra Trees Classifier
Mean of : 0.896	(+/-) 0.001	Bagging KNeighbors Classifier
Mean of : 0.945	(+/-) 0.001	Bagging SVC
Mean of : 0.936	(+/-) 0.001	Bagging Ridge Classifier
Mean of : 0.968	(+/-) 0.015	Bagging Ensemble

Table.2 (b). Improvement in Boosting Accuracy

Accuracy	**Standard deviation(**std**)**	**Classifier**
Mean of: 0.952	(+/-) 0.015	Random Forest Classifier

Mean of: 0.888	(+/-) 0.014	Extra Trees Classifier
Mean of: 0.883	(+/-) 0.014	KNeighbors Classifier
Mean of: 0.956	(+/-) 0.001	SVC
Mean of: 0.938	(+/-) 0.005	Ridge Classifier
Mean of: 0.97.6	(+/-) 0.04	Ensemble

We have improved the accuracy (0.978 vs 0.976 and decreased the variance (std: (+/-) 0.015 against. Std: (+/- 0.04) so that we function according to our ensemble modelling by integrating all the different models in one.

Table.3. Performance analysis of our conceptual model

Accuracy	Standard	Classifier
0.95	(+/- 0.01)	Random Forest
0.88	(+/- 0.01)	Extra Trees
0.88	(+/- 0.01)	KNeighbors
0.956	(+/- 0.00)	SVC
0.938	(+/- 0.01)	Ridge Classifier
0.97	(+/- 0.01)	Ensemble

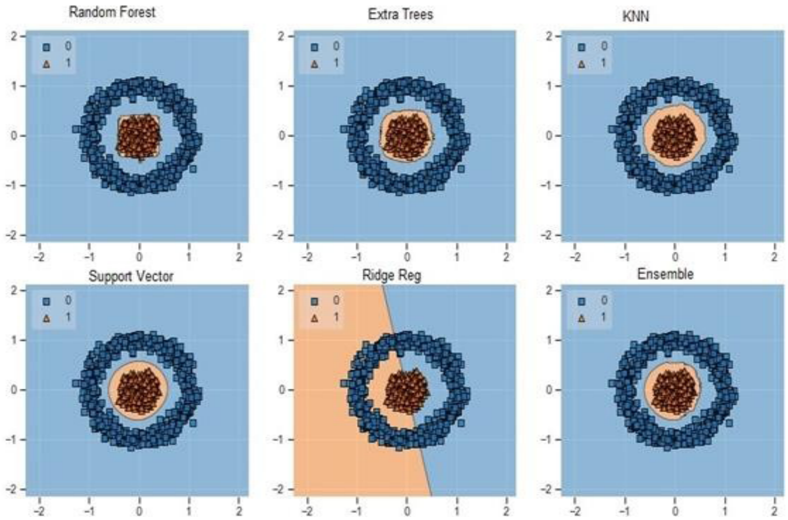


Fig.2. Classifiers on plot decision regions

Performance Analysis of Our Conceptual Meta-Ensemble Platform (Design)

From the findings of the last section, it is understandable that applying various outputs of different classifiers improves classification accuracy over the current independent classifier in the combination. Nonetheless, it does not do as well as boost—the values by optimizing processes specifically to minimize the value of errors, thus integrating works indirectly. Since our proposed model works so well to generate the best results from the combination, we have used this approach to combine our ensemble results with boost performance, stacking, andBagging and form a meta-ensemble architecture platform Fig. 1 and Fig. 3.

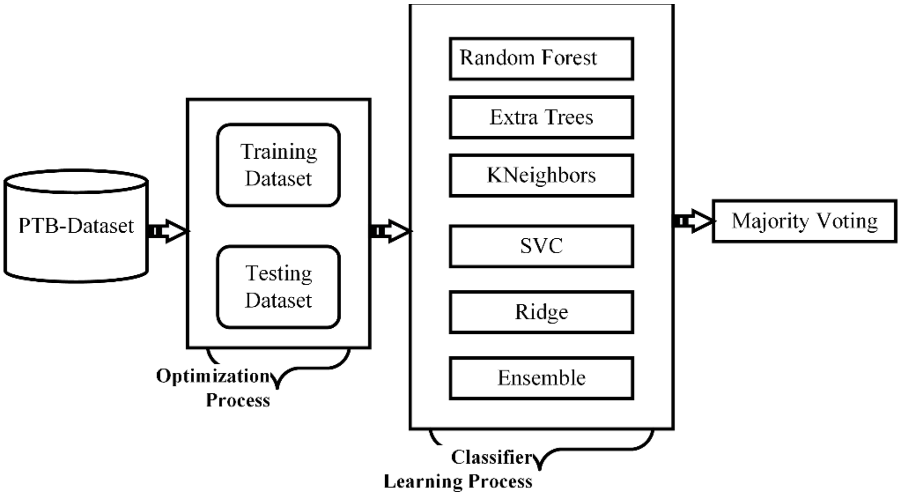
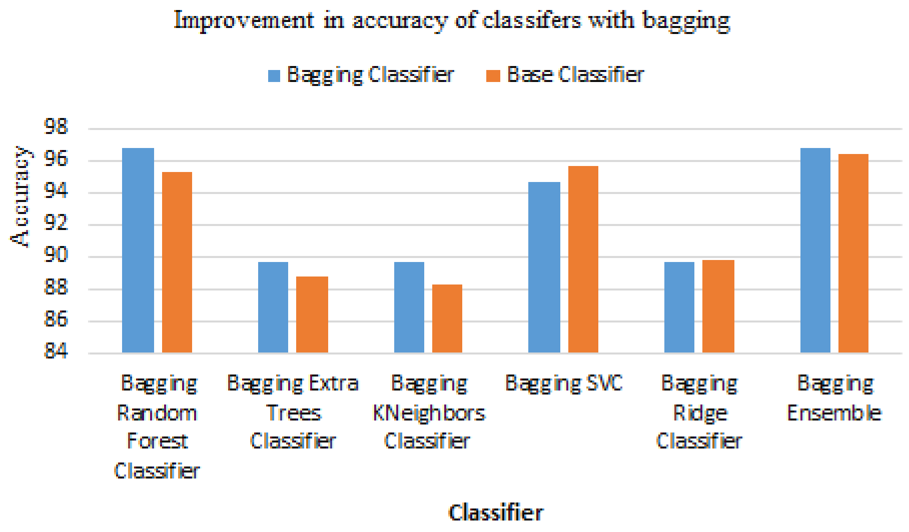


Fig.3. The ensemble voting architecture

The experimental results show that our model is better in most situations than choosing the best classifier in the combined effect. We have also proposed an effective way of combining the ensemble's classification outcomes, but it depends on each classifier class outputs in the combined [23]. The experimental findings demonstrate that our approach performs better in certain cases than choosing the most appropriate single classification. Therefore, our model is tested in this way on a single class dataset.

A comparative analysis has been made on the original dataset of various classification algorithms. Some algorithms are highly accurate, although some have limited performance. Ensemble algorithms are used to increase the efficiency of the weak classifiers. This research used algorithms to enhance voting, boosting, and stacking, including Bagging. The Bagging algorithm executes an ensemble with the Bagging Random Forest Classifier, Bagging ExtraTrees Classifier, Bagging KNeighbors Classifier, and Bagging SVC, Bagging Ridge Classifier algorithms for boosting. For this experiment, sets are generated using the Random Forest Classifier, ExtraTrees Classifier, KNeighbors Classifier Bagging, and SVC Sacking Classifier for boosting use. Machine learning algorithm. Much of the votes has often been included as ensemble techniques.



Voting through the majority is another ensemble strategy that combines several classifications for improved accuracy [23]. In this proposed model, the GaussianNB classifier weak classifiers for the original dataset and less accuracy. Ridge Classifier and Random Forest performed well and had better classification accuracy. It is inferred from Fig. 4 that a party of weak classifiers with high majority vote classifiers significantly increases the accuracyof a weak classifier. Ensemble multilayer perceptron, Gradient Boosting, and SVM improved the accuracy of strong classifiers.

Fig.4. bagging classifiers accuracy Improvement

Bagging and boosting enhancing comparative analysis are seen in Fig.4. The findings indicate that both Bagging and boosting weak classifiers are useful to increase the accuracy of weak classifiers. The calculation period is measured as the sum of 100 loops, and the value is in seconds. There is a measure of the classifier comparable estimation period for bagging and boosting methods are shown in Table.4.

Table.4. bagging and boosting computing time comparison

Classification Algorithm	Run time	Stacking Run time	Bagging Run time
KNeighbors	0.221157	0.299157	0.288229
Random Forest	1.886573	0.656246	0.699129
GaussianNB	0.046866	0.082776	0.072806
Extra Trees	1.870072	0.616354	0.583439
SVM	0.717640	2.108359	2.074450
Ridge Classifier	0.062484	0.080791	0.094748
Logistic Regression	0.527627	0.274266	0.270278

Decision Boundaries

The decision method was developed by Kuncheva. In this approach, the expected outcome of the classifiers oninstance x is organized in the decision method as the matrix.

$$\mathrm{h}i^{1}(x) \quad \mathrm{h}□\,(x) \quad \mathrm{h}□\,(x)$$

$$DP(x) = (\mathrm{h}□\,^{1}(x) \;\; \mathrm{h}□\,□\,(x)\mathrm{h}□\,□\,(x) \;\;)\,\mathrm{h}□\,^{1}(x)$$
$$\mathrm{h}□\,□\,(\mathrm{x}) \;\; \mathrm{h}□\,□\,(\mathrm{x})$$

Based on the training data set D = $\{(\,x\;,\,)\ldots\ldots\ldots(\,x□\;\;,\,y□\,)\}$, the decision approach is estimated as the expected

DP(x). Ie.

DT□ = ∑ DP(x), k $=$ 1 … . . , I

Boosting on the optimization

Boosting uses a different re-sampling method. The sample selection is based on a current training dataset in this scenario. The initial dataset is the first classification in which each sample has equal weight (Fig. 5). The weight will be reduced when the sample has properly been classified in the previous training data set; otherwise, it will increase if the sample is misclassified [23]. The committee choice uses a weighted voting technique to ensure a more accurate classification is given a higher weighting than a less accurate classification in shown Fig.5.

This optimization can be overcome for gradient descent, and gradient Vanilla is used to reduce the number of parameters. Estimating parameters appears easy if we have a smoother convex parameter, but not all problems make such an easy path. Our problem is that it generates a dynamic gradient with many categorical and binary variables and local minima to hold in during the optimization process. It can use a different type of descent calledboosting for these problems.

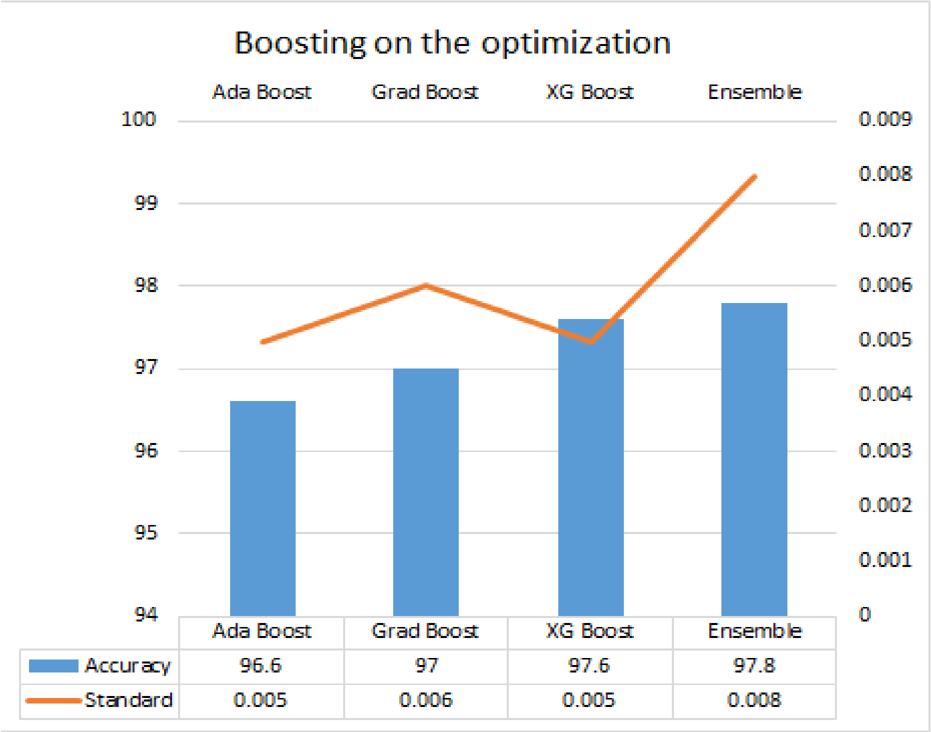


Fig.5 Performance of Boosting Analysis

Ada Boost

AdaBoost's algorithm is a linear combination of a "simple" "weak" classifier for the building of a "strong" classifier. Rather than re-sampling, each sample uses a weight to measure the likelihood of selecting a training set.

The final classified algorithm is based upon weighted voting by the weak classifiers. This classifier is more sensitive to noisy data and outliers [18, 23]. Nevertheless, it may be less exposed to overfitting in certain challenges than other learning algorithms.

Machine learning classifiers for Stacking

The machine learning (ML) algorithm ensemble uses gradient-enhancing decision-makers, which depend on the combination of weak individual classifier's performance [25]. That model consists of decision trees with logical structures and a leaf describing a weight of probability [26]. With dichotomous attributes, directions differ from "yes" (present) to "no" (absences) replies; and for continual attributes, cutoffs have decision-making restrictions to guide pathways. The final probability estimate is the total weight of all trees in the model.

Stacking

Stacking is a technique used to combine many classification models through a Meta classifier. The multiple layers are arranged one by one. Each model converts its predictions into the above model, and the top layer model takesdecisions based on the following models below. The result shown from the original data set is given to the bottomlayer models [18, 23].

The fundamental concept is to train first-level learners using learner training data sets and create a new dataset for second-level learners. First-level learner performance is still called input features. At the same time, the original labels continue to be seen as new training data labels. The first-level learners are often created by applying differentstudy algorithms so that stacked classes are often heterogeneous. However, they can also create homogenous stacked classes [23].

```
Let D= {bs-□ , bs□ , b-□ , bs-□ , bs-□ .......bs-□ } be the given dataset E = {E□ , E□ , E□ ,......E□ }, the set of ensemble classifiers

C = {c□ , c□ , c□ ...     c□ }, the classifiers

X = the training set, X□  D Y = the test set, Y □  D

L = n (D)

For I = I to L do

M (I) = Model trained using E (i) on XNext i

M=M ∪K

Result = Y classified by M
```

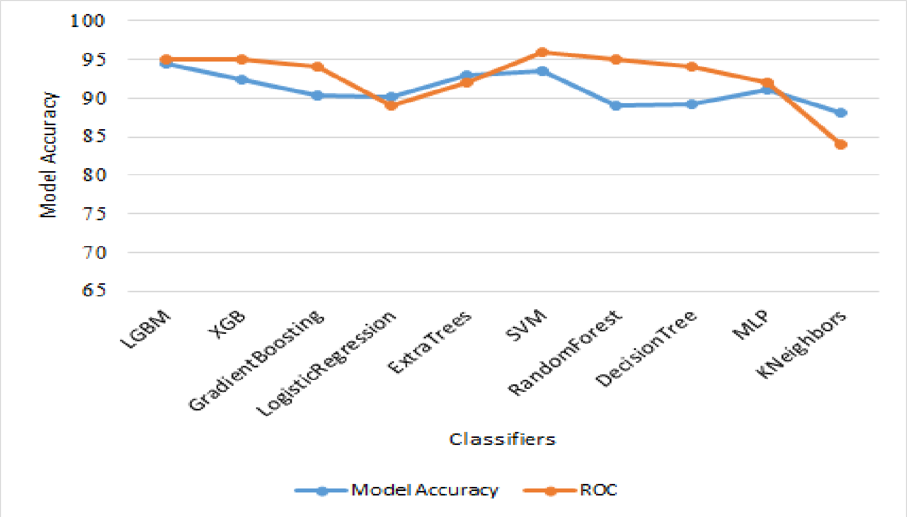
The pseudo-code of the stacking algorithm.

It has been designed to measure the performance of a model for computational analysis. Boosting is one of the ensemble approaches to adjust the errors of the existing model and to improve the new model [27]. Recurrent versions should be introduced before no major changes can be made. Boosting algorithm is designed to create a new model that predicts the residuals of prior models and then is added together to make the final prediction. A descent algorithm significantly reduces failure when new models are implemented. This method encourages classification and regression, and efficiency has changed significantly [25]. This algorithm has been published in the library of Python SciKit-learn and comes with new regularization techniques. The model must be closely configured to obtain optimum efficiency. A tuning boost can be an extremely challenging process due to its hyperparameter level. Such parameters may be divided into general parameters booster, analysis function, and command line. A grid search will do tuning.

This study uses an optimal grid method with a large parameter size. This method can effectively be achieved by integrating parameters with rational parametric values in a smaller combination. In the selection process, K- cross- validation is used to test the model's consistency [24, 25]. Python modules and resources for our simulation for research. The model achieved the performance of a true positive rate is high, false discovery rate low, and F1 score test with ten-fold cross-validations. Our proposed model automatically performed better than existing models based on machine learning.

Table.5. performance of stacking classifiers

Accuracy	Standard	Classifier
0.84	(+/- 0.01)	KNeighbors
0.95	(+/- 0.05)	Random Forest
0.52	(+/- 0.01)	GaussianNB
0.93	(+/- 0.04)	ExtraTrees
0.935	(+/- 0.00)	SVC
0.94	(+/- 0.05)	Ridge Classifier
0.96	(+/- 0.00)	Stacking



Results indicate that certain algorithms have better efficiency of detection than others. Table.5 lists the classification methods used to predict various classifying algorithms for the best accuracy. Such measures would be the most relevant criterion for classifying the health informatics field as the best algorithm. The prediction results in precision between single classifiers, random forest and ensemble, LGBM, and Extra trees is the best. Graphically equivalent in fig.6 are other measures like F-measure and ROC of the above-noted classifiers. The average F-score and ROC of the two divisions are seen. These classifiers are seen in fig.7 for prediction accuracy.

Fg.6. Comparison of average F-score and ROC area

The ROC curve is a descriptive plot determining a binary classifier frame's predictive efficiency, as its threshold edge has fluctuated. The ROC curve is made by plotting the true positive rate (TPR) against the false positive rate (FPR) at different limit settings. The true positive rate is sensitivity. For machine learning, the true positive increase is considered sensitive. Otherwise, the false positivity rate is considered the drop-out or possibility of a negative outcome (1-specificity). The ROC curves and the proposed model for the baseline classifier are related. The ROCcurve takes False Positive Rate indicating the ratio of the wrong classification on positive class, and the percentageof correct classification on positive class, indicating True Positive rate. The ROC curve shows the likelihood thata true positive instance will be better estimated than an actual negative instance by the classifier. As the classification efficiency is strong, the complete ROC curves for the baseline classifier seen on the PTB original data set, the proposed model, and the diagnostic model accuracy measures are in Fig.6 and Fig.7.

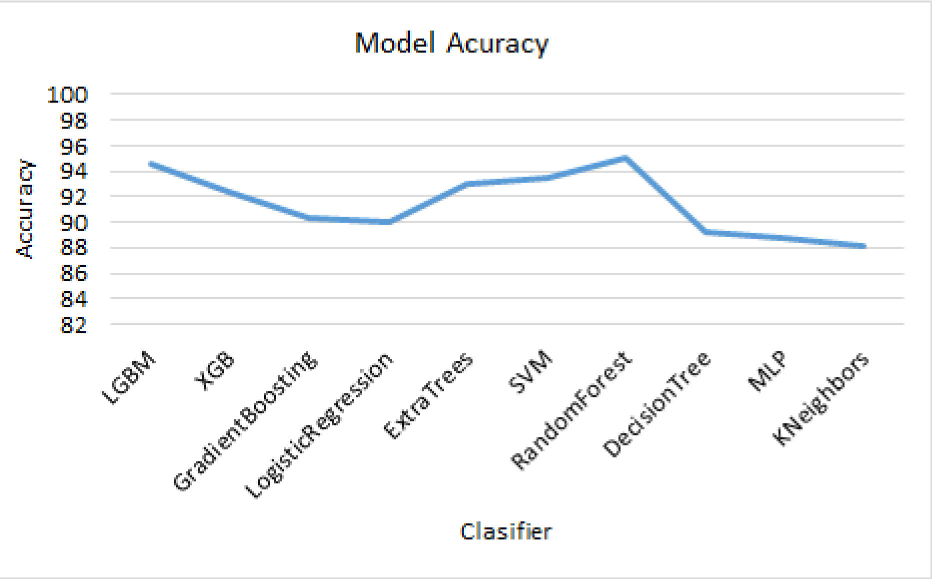


Fig. 7. comparing the prediction accuracy of all classifiers

CONCLUSIONS

In this research study, we propose to improve the consistency of the classification of a data integration ensemble model. We conclude that applying the functional specification for the building and configuration of the model nominated improves its accuracy. Currently, tuberculosis-artificial analytical know-how has not been acquired, and thus a clinical diagnosis remains needed to conclude that this method has achieved diagnostic results. Our findings indicate that the model integrating all relevant data types effectively output performs models that considerone data type. These approaches may be transformed as better methods of incorporating state-of-the-art technologybecause several models may be used to locate details about each technology category, such that certain knowledgeis not accessible. After all, only one model category is used. Enhanced design performance methods substitute selected features with high sensitivity and low accuracy in clinical knowledge. The Ensemble model reaches 97.8% accuracy, which exceeds each classification's accuracy. The model is used to help doctors analyze & evaluate medical cases to validate the diagnosis and minimize human error. It effectively mitigates clinical diagnosis in such complex challenges as microscopic scanning and reduces the likelihood of misdiagnosis.

COMPLIANCE WITH ETHICAL STANDARDS

Conflict of interest

The corresponding author states that there is no conflict of interest.

Ethics Statement

This study was approved by the institutional review Ethics board at the Faculty of Medicine, Wolaita Sodo University, with the approval code: WSU/41/15/206 and date 5/9/019. Patients have given written consent for theuse of material for research purposes.

Ethical approval of this article does not contain any studies with human participants or animals performed by any of the authors.

Informed consent was obtained from all individual participants included in the study.

Human and animal rights this article does not include any research conducted by any of the authors with human participants or animals.

Acknowledgements

We thank the referees for Sharda University hospital and Wolaita Sodo University Teaching Referral hospital

REFERENCES

[1] Xiong, Y., Ba, X., Hou, A., Zhang, K., Chen, L., & Li, T, Automatic detection of mycobacterium tuberculosis usingartificial intelligence. *Journal of thoracic disease 10*(3) (2018) 1936. https://doi.org/10.21037/jtd.2018.01.91

[2] Alves, E., Souza Filho, J. B., & Kritski, A. L , an ensemble approach for supporting the respiratory isolation of presumed tuberculosis inpatients. *Neurocomputing 331* (2019) 289-300. https://doi.org/10.1016/j.neucom.2018.11.074

[3] Sreeramareddy, C. T., Qin, Z. Z., Satyanarayana, S., Subbaraman, R., & Pai, M, Delays in diagnosis and treatment of pulmonary Tuberculosis in India: a systematic review. *The International Journal of Tuberculosis and Lung Disease 18*(3) (2014) 255-266. https://doi.org/10.5588/ijtld.13.0585

[4] Sahli, H., Mouelhi, A., Diouani, M. F., Tlig, L., Refai, A., Landoulsi, R. B., & Essafi, M ,An advanced intelligent ELISA test for bovine tuberculosis diagnosis. *Biomedical Signal Processing and Control 46* (2018) 59-66. https://doi.org/10.1016/j.bspc.2018.05.031

[5] Sarin, R., Vohra, V., Khalid, U. K., Sharma, P. P., Chadha, V., & Sharada, M. A , Prevalence of pulmonary Tuberculosis among adults in selected slums of Delhi city. *Indian Journal of Tuberculosis 65*(2) (2018) 130-134.https://doi.org/10.1016/j.ijtb.2017.08.007

[6] Mithra, K. S., & Emmanuel, W. S, GFNN: gaussian-fuzzy-neural network for diagnosis of Tuberculosis using sputum smear microscopic images. *Journal of King Saud University-Computer and Information Sciences* (2018). https://doi.org/10.1016/j.jksuci.2018.08.004

[7] Dande, P. and Samant, P, Acquaintance to artificial neural networks and use of artificial intelligence as a diagnostic tool for Tuberculosis: a review. Tuberculosis, 108 (2018) 1-9. https://doi.org/10.1016/j.tube.2017.09.006

[8] Global Laboratory Initiative , GLI Model TB Diagnostic Algorithms (2018).

[9] Sohn, H, Improving tuberculosis diagnosis in vulnerable populations: impact and cost-effectiveness of a novel, rapid molecular assays (Doctoral dissertation, McGill University Libraries) (2016).

[10] ASHA, T., NATARAJAN, S., & MURTHY, K. B, Estimating the Statistical Significance of Classifiers used in the Prediction of Tuberculosis. *IOSR Journal of Computer Engineering (IOSRJCE)* (2012) *5*(5).

[11] Orjuela-Cañón, A. D., Mendoza, J. E. C., García, C. E. A., & Vela, E. P. V , Tuberculosis diagnosis support analysis for precarious health information systems. *Computer methods and programs in biomedicine 157* (2018) 11-17. https://doi.org/10.1016/j.cmpb.2018.01.009

[12] Jahantigh, F.F., and Ameri, H, Evaluation of TB patients characteristics based on predictive data mining approaches.

Journal of Tuberculosis Research 5(1) (2017)13-22. https://doi.org/10.4236/jtr.2017.51002

[13] Zulvia, F.E., Kuo, R.J. and Roflin, E, An Initial Screening Method for Tuberculosis Diseases Using a Multi-objective Gradient Evolution-Based Support Vector Machine and C5. 0 Decision Tree. In 2017 IEEE 41st Annual Computer Software and Applications Conference (COMPSAC). IEEE, 2 (2017)

204-209. https://doi.org/10.1109/COMPSAC.2017.57

[14] Wu, Y., Wang, H. and Wu, F , Automatic classification of pulmonary Tuberculosis and sarcoidosis based on random forest. In 2017 10th International Congress on Image and Signal Processing, Bio-Medical Engineering and Informatics (CISP-BMEI). IEEE, (2017) 1-5. https://doi.org/10.1109/CISP-BMEI.2017.8302280

[15] Orjuela-Cañón, A.D., Mendoza, J.E.C., García, C.E.A. and Vela, E.P.V , Tuberculosis diagnosis support analysis forprecarious health information systems.Computer methods and programs in biomedicine, 157 (2018) 11-17. https://doi.org/10.1016/j.cmpb.2018.01.009

[16] Benbelkacem, S., Atmani, B. and Benamina, M, Treatment tuberculosis retrieval using a decision tree. In 2013International Conference on Control, Decision and Information Technologies (CoDIT). IEEE, (2013) 283-288. https://doi.org/10.1109/CoDIT.2013.6689558

[17] Alves, E.D.S., Souza Filho, J.B., Galliez, R.M. and Kritski, A, Specialized MLP classifiers to support the isolation of patients suspected of pulmonary Tuberculosis. In 2013 BRICS Congress on Computational Intelligence and the 11th Brazilian Congress on Computational Intelligence. IEEE, (2013) 40-45. https://doi.org/10.1109/BRICS-CCI-

CBIC.2013.18

[18] Schwenker, F, Ensemble methods: Foundations and algorithms [book review]. *IEEE Computational IntelligenceMagazine 8*(1) (2013) 77-79. https://doi.org/10.1109/MCI.2012.2228600

[19] Ren, Y., Zhang, L., & Suganthan, P. N, Ensemble classification and regression-recent developments, applications andfuture directions. *IEEE Computational intelligence magazine 11*(1) (2016) 41-53. https://doi.org/10.1109/MCI.2015.2471235

[20] Shah, S. M. S., Batool, S., Khan, I., Ashraf, M. U., Abbas, S. H., & Hussain, S. A, Feature extraction through parallelprobabilistic principal component analysis for heart disease diagnosis. *Physica A: Statistical Mechanics and its Applications 482* (2017) 796-807. https://doi.org/10.1016/j.physa.2017.04.113

[21] Yu, L., & Liu, H. , Feature selection for high-dimensional data: A fast correlation-based filter solution. In *Proceedingsof the 20th international conference on machine learning (ICML-03)*, (2003) 856-863.

[22] Bania, R. K., & Halder, A, R-Ensemble: A greedy rough set based ensemble attribute selection algorithm with kNN imputation for classification of medical data. *Computer Methods and Programs in Biomedicine 184* (2020) 105122.https://doi.org/10.1016/j.cmpb.2019.105122

[23] Zhou, Z. H, Ensemble methods: foundations and algorithms. CRC press (2012).

[24] Syafrullah, M, Diagnosis of Smear-Negative Pulmonary Tuberculosis using Ensemble Method: A Preliminary Research. In 2019 6th International Conference on Electrical Engineering, Computer Science

and Informatics (EECSI).

IEEE, (2019) 112-116. https://doi.org/ 10.23919/EECSI48112.2019.8976920

[25] Kim, J., Chang, H., Kim, D., Jang, D. H., Park, I., & Kim, K, Machine learning for prediction of septic shock at initialtriage in the emergency department. *Journal of critical care 55* (2020) 163-170. https://doi.org/10.1016/j.jcrc.2019.09.024

[26] Evora, LHRA, Seixas, JM and Kritski, A.L, Neural network models for supporting drug and multidrug-resistant tuberculosis screening diagnosis. Neurocomputing, 265(2017) 116-126. https://doi.org/10.1016/j.neucom.2016.08.151

[27] Xiong, Y., Ba, X., Hou, A., Zhang, K., Chen, L., & Li, T, Automatic detection of mycobacterium tuberculosis usingartificial intelligence. *Journal of thoracic disease 10*(3) (2018) 1936. https://doi.org/ 10.21037/jtd.2018.01.91

27

NET NEUTRALITY: NEED FOR A LEVEL GROUND FOR ALL PLAYERS

KEYWORDS

NET-NEUTRALITY, ISPS, TRAI, INDIA, OPEN INTERNET, CONSUMERS OF THE INTERNET, EQUAL INTERNET ACCESS

CHAPTER TWENTY SEVEN

NET NEUTRALITY: NEED FOR A LEVEL GROUND FOR ALL PLAYERS

AUTHOR

SONU CHOUDHARY, LL.M STUDENT, NLU RANCHI

ABSTRACT

Technology in recent times has reformed the world economy and has drastically increased the economic accessibility, prompted the progression of the business community. Given the traumatic pandemic of Novel Covid-19, technology as inasmuch easy access to the internet has brought the world together to overcome the pandemic, be it business, imparting education, governance and above all being catered of daily needs of a common citizen. Unfolding the usage of the internet, postulate being put forth is the Right to have Equal Access to the Internet as a Fundamental Right encompassing Article 21 of Indian Constitution and further unfolds the ongoing debate of Net Neutrality. This research paper discusses the concept of net neutrality in India and around the major developed countries outlining the historical background leading to the development of various regulations. Further, given the corporate being involved in an in-depth data scam, bluntly violating the net neutrality norms, this paper focuses on India's perspective regarding net neutrality by highlighting various regulations, debates and licensing norms for ISPs and its stand. Further, it highlights major economies such as the US and the EU model of net neutrality and their official stand or norms to regulate internet services. Lastly, conclude the research paper by critically analysing stakeholders of ISP's not being in favour of net neutrality and

the urgent need for Net Neutrality Legislation in India for the protection of rights for consumers of Internet.

INTRODUCTION

"Net neutrality (network neutrality, Internet neutrality, or net equality) is the principle that internet service providers and governments should treat all data on the internet the same, not discriminating or charging differentially by user, content, site, platform, application, type of attached equipment, or mode of communication"[1]. "*The term was coined by Columbia University media law professor Tim Wu in 2003, as an extension of the longstanding concept of a common carrier*"[2]. However, "Wu made it clear that it was not total non-interference that he was advocating; rather, he factored in the Harm Requirement that is ISPs[3] were allowed to discriminate on content when the user's use was publicly detrimental or caused public harm"[4].

The concept of net neutrality cannot be equated with the fact of blocking of content. "Interference also includes the ISPs prioritizing certain data over other –a situation wherein the ISP can categorise certain content as high-priority, and choose to forward it first, as opposed to operating on a first-come-first-served basis"[5].

Net neutrality discussed largely two non-discrimination propositions – "First, that Internet users should have access to all content on the internet, unregulated by any ISP and second, that a higher Quality of Service for a higher price be offered to users on fair, reasonable and non-discriminatory terms"[6].

In the 1980s and 1990s the time period when the internet started to explore, this principle of net neutrality was not in existence as there were no specific rules regarding the same whereas telecom operators act like ISPs (Internet Service providers), they abide by this principle.

BACKGROUND

Development between the Era of 2006 – 2013

In 2006, TRAI welcomed viewpoints with respect to the guideline of net neutrality from different telecom industries and partners. It was noticed in the year 2006 when TRAI distributed a counsel paper the fact that since 1998, the Internet had been nonpartisan and private ISPs were permitted to start the tasks but the circumstance

[1] Available at https://corporatefinanceinstitute.com/resources/knowledge/other/net-neutrality/ visited on January 10, 2022

[2] Tim Wu, A Proposal for Network Neutrality, 1, available at http://www.timwu.org/OriginalNNProposal.pdf?, visited on January 10, 2022

[3] **Internet service provider (ISP),** company that provides Internet connections and services to individuals and organizations. The Editors of Encyclopaedia Britannica, *Internet service provider,* Encyclopædia Britannica (March 13, 2018).

[4] T. Wu. Network Neutrality, Broadband Discrimination. Journal of Telecommunications and High Technology Law, 2:141, 2003

[5] Edward, W. Felton, Nuts and Bolts of Network Neutrality, 3 available at http://regulation2point0.org/wp-content/uploads/downloads/2010/04/php9e.pdf, visited on January 10, 2022.

[6] Christopher T. Marsden, Network Neutrality and Internet Service Provider Liability Regulation: Are the Wise Monkeys of Cyberspace Becoming Stupid? , 2(1) GLOBAL POLICY 2(2010).

may alter later on as Internet Service Providers engaging in victimize contending applications and substance suppliers. This leads to influencing the administrations like Internet communication and services like Internet telephony. "The paper invited opinions from stakeholders on whether the regulatory intervention was required or whether it should be left to market forces"[7].

Further different development seen in this area as around 2012, the CEO of Bharti Airtel, Sunil Bharti Mittal at the World Mobile Congress held in Barcelona proposed that in the event where telecom administrators are building interstates for information, the operators like YouTube should pay an interconnect charge as they are ought to be on a duty on the parkway. In the same line of thought Bharti Airtel's Director of Network Services, Jagbir Singh, recommended that huge Internet organizations like Facebook and Google should impart incomes to telecom organizations. "According to him, Internet companies were making big profits from small investments, whereas telecom companies were investing in building networks. He also suggested that the telecom regulator should establish interconnection charges for data services, similar to those applied to voice calls"[8].

The issue of ISPs choking Internet traffic, be that as it may, isn't new. Well known U.S ISP Comcast went under the spotlight in 2007 for impeding Bit Torrent traffic, which brought about controversy. The Federal Communications Commission imposed a fine of around $16 million to ISPs and at last decided that Comcast needed to stop its focus on induction of clients' Bit Torrent traffic. "In February 2013, Killi Kruparani, Union Minister of State for Communications and Information Technology, said that the government would look into the legality of VoIP services"[9]. "The Chief General Manager of the state-run BSNL, V. Srinivasan also said that services like Skype are illegal"[10].

Development in the Era of 2014

To regulate the service providers and their services, different instances were observed during this era of 2014. Mr Gopal Vittal, the CEO of Airtel's India operations in February, stated that the organizations involved in offering free information applications like Skype, Line and WhatsApp ought to be controlled in a similar fashion like telecom administrators. But TRAI dismissed a proposition in August 2014 from telecom organizations to make informed application firms share part of their income with the transporters or the public authority.

In October Vodafone India CEO Marten Pieters, proposed the suggestion for giant organizations such as Facebook and WhatsApp to be treated similarly as the telecom operators by stating that these organizations ought to be burdened to guarantee a level battleground. At the same time, TRAI started an investigation against Airtel whether Airtel offered particular plans by offering exceptional net packs where WhatsApp and Facebook app rates were lower than its standard information rates. Even in December case reported against Airtel where

[7] "Consultation Paper on Review of Internet Service" *(PDF).* Telecom Regulatory Authority of India *(TRAI).*

[8] "Google, Facebook should share revenue with us: Airtel". The Hindu Business Line. *20 July 2012.*

[9] "VoIP is an acronym for Voice over Internet Protocol that describes the method to place and receive phone calls over the internet, considered as an alternative to the local telephone company it includes services such as auto attendants, call recording, custom caller ID, voicemail to email, and so much more. One can take calls and work from anywhere" Yaniv Masjedi, What Is VoIP & How Does It Work?, Nextiva Blog (October 12, 2020)

[10] "As debate over Net telephony rages, Govt to re-examine services offered by Skype, Google". The Hindu Business Line. *11 February 2013.*

Airtel asked for extra charges for settling on voice calls (VoIP) from its organization utilizing applications like Skype, WhatsApp, and so on as Airtel changed its plans for those using 2G and 3G information packs so that VoIP information would be exempted from the set measure of free information.

These instances initiated the discussion on internet fairness in India. On this issue or instances, Mr Rahul Khullar chief of the TRAI stated that Airtel can't be considered answerable for abusing internet fairness since India has no guideline that requests internet fairness. Airtel's move confronted analysis on interpersonal interaction destinations like Facebook, Twitter and Reddit. He added that what Airtel attempted to do was against internet fairness, yet not illicit, as India had not come up with any law or statute which authorizes internet fairness. "From this stage, TRAI explores this aspect by initiating a consultation paper on regulating OTT services to level the playing field. OTT firms will have to apply for licenses and share revenue with the government"[11].

In November 2014, US President Barack Obama also came in support of Net Neutrality, encouraging the FCC (Federal Communications Commission) to execute the most grounded potential guidelines to secure net neutrality and guarantee that "neither the cable company nor the phone company will be able to act as a gatekeeper, restricting what you can do or see online". He likewise referenced that FCC should make these guidelines completely material to mobile broadband too, because of the expanding appropriation of cell phones to get to the Internet. He likewise requested that FCC rename shopper broadband assistance as a public utility.

Development in the Era of 2015-2018

"In January 2017, President Trump appointed Republican FCC Commissioner Ajit Pai as the agency's new chair and he announced a plan to reverse the 2015 net neutrality order but in December 2017 FCC voted effectively against the 2015 rules in their entirety. The FCC's new rules drop the common-carrier status for broadband providers, as well as any restrictions on blocking or throttling content"[12]. To regulate these exemptions or restrictions, the new rules framed and as per rules, there should be full disclosure of their network-management practices by the internet service providers. It is now the responsibility of the Federal Trade Commission[13] to protect the interest of consumers from any violations of the net neutrality principle.

India took two major steps during the period 2016-2018, towards establishing the most powerful or rigid structure for the principle of net neutrality in the whole world.

"The first step, taken by the Telecom Regulatory Authority of India (TRAI) in February 2016, was the adoption of a regulation[14] to prohibit any content-based pricing of data services[15]. This raised serious concerns about the

[11] "Airtel move to charge VoIP calls not illegal: TRAI chief Rahul Khullar". The Indian Express. *27 December 2014*.

[12] lint Finley, *The WIRED Guide to Net Neutrality,* Wired (May 5, 2020) available at https://www.wired.com/story/guide-net-neutrality/

[13] The FTC is only an enforcement agency: It can't create new rules. That means that unless a net neutrality violation is also illegal under existing fair-competition laws, there's not much the agency can do about it. Outright blocking a competitor may well be an antitrust violation, but creating fast lanes for companies that pay extra for special treatment might not be.

[14] Prohibition Of Discriminatory Tariffs for Data Services Regulations, 2016 (No.2 of 2016) https://trai.gov.in/sites/default/files/Regulation_Data_Service.pdf

[15] This decision was the resultant of the tie-up between Facebook and Reliance Communications for introducing the Free Basics platform.

Internet being splintered into free and paid versions, with accompanying negative effects for online innovation and free speech and the second step adopted by the Indian government in July 2018 to adopt a comprehensive set of principles on non-discriminatory[16] access to content”[17].

NET NEUTRALITY IN INDIA: PRESENT SCENARIO

Net Neutrality Legislation and Regulations

“At present, there is no specific legislation governing Net Neutrality in India which would require that all Internet users be treated equally, without discriminating or charging differentially by user, content, site, platform, application, type of attached equipment, or mode of communication”[18] but TRAI brought various regulations to regulate the internet related issues. There are a plethora of instances as discussed above the violations principle of net neutrality by various Indian service providers like Aircel’s free access to Facebook and WhatsApp, Airtel zero scheme, Aircel’s Wikipedia zero, Facebook’s internet.org, etc.

“In March 2015, Telecom Regulatory Authority of India (TRAI) released a formal consultation paper on *Regulatory Framework for Over-the-top (OTT)* services[19], seeking comments from the public”[20] . “Finally, TRAI released *the Prohibition of Discriminatory Tariffs for Data Services Regulations, 2016 on 08.02.2016”*[21].

“These Regulations state that no service provider is allowed to enter into any agreement or contract that would result in discriminatory tariffs being charged to a consumer based on content (data services)”[22]. Meanwhile, the Cellular Operators Association of India (COAI) launched a program termed *Sabka Internet, Sab ka Vikas*. “It claimed that COAI members aim to connect the unconnected citizens of India and demanded that VoIP apps should be treated as cellular operators”[23].

“TRAI reviews these regulations after two years and In November 2017, TRAI recommended that the license agreement entered into between the Government and ISPs should be amended to clarify that ISPs are not permitted to discriminate between different types of content on the Internet, including based on factors such as the sender or receiver of the data packets, the protocols being deployed or the equipment being used. This

[16] This decision imposes restriction on Internet service providers (ISPs) from imposing any kind of discriminatory treatment on the basis of content.

[17] Smriti Parsheera , *Net Neutrality In India: From Rules To Enforcement,* Medianama (May 18,2020). Available at https://www.medianama.com/2020/05/223-net-neutrality-india-rules-enforcement/

[18] Apoorva, The Net Neturality Debate in India, PRS Legialtive Reserch (February 9,2016) https://www.prsindia.org/theprsblog/net-neutrality-debate-india

[19] “Over the top (OTT) refers to film and television content provided via a high-speed Internet connection rather than a cable or satellite provider. Viewers who dislike paying for bundled content are often referred to as cord cutters. OTT does not mean free, as the term encompasses services such as Netflix, Amazon, iTunes and HBO Now”

[20] “Consultation Paper On Regulatory Framework for Over - the - top (OTT) services” *(PDF).* Telecom Regulatory Authority of India. *27 March 2015* visited on January 11, 2022.

[21] *Supra* note 12

[22] Venancio D’Costa and Astha Ojha, *Net Neutrality In India: Regulating Evolving Technology,* Mondaq (14 August 2020) available at https://www.mondaq.com/india/telecoms-mobile-cable-communications/976168/net-neutrality-in-india-regulating-evolving-technology

[23] Lalatendu Mishra, *War of words over net neutrality continues*, The Hindu (September 6, 2016) available at https://www.thehindu.com/news/national/war-of-words-over-net-neutrality-continues/article7171675.ece

recommendation came to be known as TRAI, 2017"[24].

"Finally, DoT on 31.07.2018 released the Regulatory framework on Net Neutrality and the said Regulations provide for the principle of non-discriminatory treatment, as per which, DoT has decided to amend the terms of various licenses governing the provision of Internet Service in India"[25].

India's Licensing Norms

Although no specific legislation or statute on net neutrality exists in India, but traces of this **c**oncept or principle are observed in the license agreements where ISPs are required to adhere to the license rules and regulations for providing services in Indian jurisdiction. As per the license agreement[26]between the ISPs and DoT, "which grants the right to supply internet services, stipulates that full compliance with the terms and conditions of the license agreement is a prerequisite to be granted an ISP license in India"[27]. The Central Government have the right to renounce an ISP's permit where ISP involves in violation of the rules and regulations of the same.

"Clause 2.2 of the License Agreement stipulates that the internet access service provided by India to its consumers must provide access to all content available on the internet"[28].

"Clause 10.7 makes it the responsibility of the ISPs to maintain the Quality of Service, and under *Clause 25.1* of the License Agreement, ISPS are bound to adhere to the QoS Regulations as prescribed by the TRAI"[29]. Moreover, the ISPs have to guarantee the Quality of various Services provided by them and hence, as per the terms of the permit, ISPS are under obligation to unmistakably characterize the extent of administration to the supporters at the time of contract

Clause 32.1 of the Agreement also states the obligation on the ISP to "ensure the protection of privacy of communication and to ensure that unauthorised interception of message does not take place".

Although "*Clause 8(xvi)* of the guidelines and general information for grant of licence for operating internet services orders ISPs to ensure that the necessary hardware and software is available with them for lawful monitoring and interception, it is submitted that this activity is restricted to the Government only, and prohibited to private parties through sub-clauses (xiii) to (xix)" [30]. Moreover, *Clause 8(iv)* also commands that the licensee will "take sufficient and convenient measures to guarantee that the data executed through an organization by the endorsers is secure and ensured", consequently re-repeating the commitment to the standards of net neutrality.

Thus, in theory, the authorizing standards in India align with and even energize the standards or principles to

[24] Venancio D'Costa Supra note 20

[25] Recommendations On Net Neutrality, TRAI (28 November, 2017) Available at https://www.trai.gov.in/sites/default/files/Recommendations_NN_2017_11_28.pdf

[26] License Agreement for the Provision of Internet Services, available at http://www.dot.gov.in/isp/internet-licence-dated%2016-10-2007.pdf , visited on January 11, 2022.

[27] Clause 3 of the License Agreement.

[28] ISP's (Terms and conditions). Available at https://techlawtopia.com/isp/ visited on January 13, 2022

[29] *Id*

[30] Guidelines and General Information for Grant of Licence for Operating Internet Services, No.820-1/2006-LR(24th Aug., 2007), available at http://www.dot.gov.in/internet%20services/internetservices.htm visited on January 11, 2022

maintain the sanctity of net neutrality. Notwithstanding, no ISP has endured sanctions or their permits were rejected on the ground of violating this standard by the TRAI Act. Consequently, it is high time for India to adopt a complete enactment for encouraging unhindered internet standards.

India's Formal Position

Around 2011, "India made its stance on Internet Neutrality clear at the 66th Session of the UN General Assembly. India recognised that the Internet was an unprecedented global medium that should be inclusive, democratic, participatory, multilateral and transparent"[31] .

"India pointed out that the Internet had grown in size and scope, and the task of Internet governance required quick-footed and timely global solutions and policies, not divergent and fragmented national policies"[32].

"It was to forward this agenda of internet governance that India suggested the setting up of a multilateral, democratic, participative and transparent global policy-making mechanism, to be known as the United Nations Committee for Internet-Related Policies (CIRP)"[33]. "The 50-member body proposed by India would be undertaking tasks such as establishing public policy as regards internet-related issues and addressing developmental issues connected to the interwebs"[34].

India gave admonitions in the report itself by expressing that this ought not to be viewed or considered as the endeavour of authority or the concerned governments to "dominate" or direct the working standard of the Internet, although media have seen this measure of the government with some venturing to such an extreme as to term it an opportunity attack. Nonetheless, different researchers have perceived the significance of this proposition –, best-case scenario, the CIRP, a multi-partner body, would democratize choices identifying with web administration, ensuring that neither the US Government nor super severe state such as China, would have the option to settle on choices over directing web content; to say the least, regardless of whether the body ended up being overwhelmed by Governments, it would bring about a more straightforward dynamic cycle and systems identified with overseeing the web. While honourable Supreme Court in the case of "*Association of*

[31] Digvijay Singh, *India's proposal for a United Nations Committee for Internet-Related Policies (CIRP),* 66th Session of the UN General Assembly, 26th Oct. 2011, available at http://www.itforchange.net/sites/default/files/ITfC/india_un_cirp_proposal_20111026.pdf visited on January 12, 2022

[32] Mishi Choudhary , *Responses to the Consultation Paper on Cloud Computing*, SFLC (July 25, 2016)

[33] "The CIRP shall be mandated to undertake the following tasks:

i. Develop and establish international public policies with a view to ensuring coordination and coherence in crosscutting Internet related global issues;

ii. Coordinate and oversee the bodies responsible for technical and operational functioning of the Internet, including global standards setting;

iii. Facilitate negotiation of treaties, conventions and agreements on Internet related public policies;

iv. Address developmental issues related to the Internet;

v. Promote the promotion and protection of all human rights, namely, civil, political, social, economic and cultural rights, including the Right to Development;

vi. Undertake arbitration and dispute resolution, where necessary; and,

vii. Crisis management in relation to the Internet" < TRAI Proposal >

[34] Available at: http://www.itforchange.net/sites/default/files/ITfC/india_un_cirp_proposal_20111026.pdf

Unified Tele-Service Providers & Ors. vs. Union of India'[35] held that

> "*State actions and actions of its agencies/instrumentalities/licensees must be for the public good to achieve the object for which it exists, the object being to serve the public good by resorting to fair and reasonable methods*"[36].

Overlooking the issues that could manifest while executing the proposition, it is imperative to observe the past violations or alleged difficulties of the concerned proposition and to analyze further the Government's goal behind this arrangement. "India has officially reaffirmed its dedication to letting the internet remain an open and transparent medium with the help of all stakeholders involved"[37].

Violations of Net Neutrality

The table below highlights the instances of the violation of the net neutrality principle under India's jurisdiction by Telecom Companies.

Year	**Company**	**Violation**
2010	**MTS**	Provided plans which allowed certain websites free internet browsing access including Wikipedia, Yahoo India, Makemytrip, shopping .indiatimes.com and Cricinfo.com.
2010	**Tata Docomo**	Offered plans where free GPRS provided for accessing apps such as Orkut, Facebook, LinkedIn, Twitter, and Nimbuzz to its Buddy Net users.
2012	**You Broadband, Airtel, and BSNL**	Throttling Bit torrent traffic
2012	**RCOM**	Offered free Whatsapp and Facebook to its GSM users for Rs 16 per month.
2013	**RCOM**	Offered free access to Twitter to its GSM customers for 90 days
2013	**RCOM**	Offered free unlimited streaming of ICC Champions Trophy 2013 on Star Sports
2013	**Airtel**	Offered free access to certain Google services to Broadband users with a limit of 1 GB of free data.
2013	**Aircel**	Offered free access to Wikipedia on the mobile phone.

[35] (2014) 6 SC 110 8

[36] *Id*

[37] The Editorial, *India's stand on net neutrality is clear, US can decide for itself: Centre*, (Dec 16, 2017) available at https://www.deccanchronicle.com/nation/current-affairs/161217/indias-stand-on-net-neutrality-is-clear-us-can-decide-for-itself-centre.html

2014	**Aircel**	Made plans under which any users who bought data packs also have the right to access apps including Facebook and WhatsApp, free of any data consumption.
2015	**Facebook**	Launched in partnership with Reliance Communications an "internet.org" which provides access to 38 websites for free through an app in India.
2015	**Airtel**	Launched Airtel zero which provides free apps to customers.
2016	**Facebook**	Facebook's Free Basics was engaged with companies to provide free access.
2017	**Airtel and Vodafone Idea**	Premium service plan.

LEGISLATIONS: INTERNATIONAL PERSPECTIVE

The United States and Net Neutrality

In 2005, FCC in its Internet Policy Statement listed the standards on Net Neutrality, which embraced various standards on the subject. Compliant with this arrangement articulation, around 2008, the FCC concluded that the ISP supplier, Comcast Corporation, had been hindering traffic for Bit torrent, the distributed sharing organization and that this training didn't establish a sensible organization for the executives. "The FCC, in its 3-to-2 decision, also ordered Comcast to end this unreasonable conduct and also required it to disclose to the Commission and the public the details of the network management practices that are intended to follow within 30 days of the Order"[38].

However, "this decision of FCC could not last long and the U.S. Court of Appeal for the District of Columbia in 2010 held that the FCC cannot exercise jurisdiction over network management of ISPs since the FCC has no ancillary authority to bar an ISP from network interference"[39] since the activity of this authority was not seen to be sensibly subordinate to the compelling exhibition of its legally commanded obligations.

In December 2010, after the Court of Appeals' choice, the FCC, for the protection of the open web passed a bunch of rules for the net neutrality principle.

These principles are-

> First, "consumers and innovators have a right to know the basic performance characteristics of their Internet access and how their network is being managed"[40].

[38] In the Matters of Formal Complaint of Free Press and Public Knowledge against Comcast Corporation for Secretly Degrading Peer-To-Peer Applications, 23 FCC Rcd. 13028 (2008)

[39] Comcast Corp. v. Federal Communications Commission, 600 F.3d 642, 390 U.S.App.D.C. 111, available at http://scholar.google.com/scholar_case?case=12158705661002658248

[40] "Adopted a transparency rule that will give consumers and innovators the clear and simple information they need to make informed choices in choosing networks or designing the next killer app"

Second, "prohibit the blocking of lawful content, apps, services, and the connection of devices to the network"[41].

Third, "consumers and innovators have a right to a level playing field"[42].

"Later rules amended due to change in government in 2015 but the Federal Communications Commission's Restored Internet Freedom Order and transparency rule amendments and due to this state legislator responded by introducing net neutrality legislation at the state level"[43].

European Union and Net Neutrality

"Around 2003 a Common Regulatory Framework for Electronic Communications ("RFEC") authorizes Federal authority dealing with electronic communications"[44].

In 2015 European Union enacted legislation on net neutrality. It aims to "*guarantee the continued functioning of the internet ecosystem as an engine of innovation by imposing net neutrality policies that prohibit any discriminatory uses of network management practices (such as blocking or throttling of lawful content) by Internet access service providers*"[45].

The key elements of this regulation are

1. Restrict Blocking: "Internet Service Providers (ISPs) shall not block lawful content, applications, services, or non-harmful devices, subject to reasonable network management"[46]
2. Restrict throttling: "ISPs shall not impair or degrade lawful Internet traffic based on Internet content, application, or service, or use of a non-harmful device, subject to reasonable network management"[47].
3. Restrict paid prioritization: ISPs shall not engage in any paid prioritization. "Paid prioritization refers to the management of a broadband provider's network to directly or indirectly favour some traffic over other traffic"[48].

"The EU operates under a generally consistent and harmonized regulatory framework; however, Member States sometimes interpret the RFEC framework in divergent ways, it is also possible for Member States to im-

[41] *Id*

[42] "No central authority, public or private, should have the power to pick winners and losers on the Internet; that's the role of the commercial market and the marketplace of ideas". Id

[43] Heather Morton, *Net Neutrality 2020 Legislation,* National Conference of State Legislature (March 27, 2020). Bottom of Form

[44] Regulatory framework for electronic communications in the European Union, European Commission (December 2009) pdf

[45] Wolfgang Briglauer, *Special Issue on 'Recent Net Neutrality Polices in Europe and the US,* Review of Network Economics Volume 17, Issue 3 (July 30, 2019) available at https://www.degruyter.com/view/journals/rne/17/3/article-p109.xml?language=en

[46] J. Scott, *New Network Neutrality Rules in Europe: Comparisons to those in the U.S. Marcus*, Colorado Technology Law Journal Vol. 14.2.

[47] *Id*

[48] *Id*

plement national laws that go beyond the RFEC in areas where the RFEC itself does not prohibit them from doing so"[49].

CONSEQUENCES

Criticism

Quite possibly the most strident evaluates of the net neutrality theory by Christopher Yoo, who states that the intermediation by ISPs can, indeed, assume a significant part in assisting clients with getting to content that they need. "Yoo waxes eloquent on the many benefits of interfering with internet content –including screening out viruses and malware at the earliest possible moment"[50], assisting clients with recognizing the substance they need to see and making answers for dealing issues opposite charges paid by clients.

Rivals of unhindered internet or net neutrality or internet neutrality additionally contend that the standards are counter-beneficial. Web traffic the board could permit touchier, significant information to be sent first – for instance, a patient's heart screen information being communicated before a video download, and hindering such the executives must be unfavourable for clients. Naysayers have additionally contended that unhindered internet just purposes development in the field of an arrangement of internet providers to drop and that internet fairness forbids ISPs from overseeing network blockage and consequently, makes the organization less proficient.

"Aside from the academic rebuttal of internet neutrality, the largest criticism of net neutrality comes from those who have the most to lose from the imposition of these principles –the profit-making ISPs"[51].

Call for Net Neutrality: Indian Jurisdiction

With the advancement or increasing number of Internet users in India, a higher chance of network congestion has been observed. In such circumstances ISPs involving in practices where they impose a particular kind of premium rent while downloading or surfing thus jeopardizing the objective of the net neutrality principle. It is critical to guarantee the non-partisanship of the Internet in the event that we need to advance reasonable rivalry and offer an opportunity to little and medium undertakings working on the Internet to develop, as these little business people won't have the option to pay higher lease to get its substance organized. Easing back down

[49] J. Scott Marcus, *Network Neutrality: Challenges and responses in the EU and in the U.S.*, www.europarl.europa.eu/RegData/etudes/etudes/join/2011/457369/IPOLIMCOET%282011%29457369_EN.pdf

[50] Christopher Yoo, *Free Speech and the Myth of the Internet as an Unintermediated Experience*, (78) George Washington L.REV. (2005) 697, 703-704.

[51] "Perhaps the best –and most honest –critique of net neutrality from the viewpoint of the ISPs can be attributed to Edward Whitacre, then the CEO of Southwestern Bell Corporation (now, AT&T) – one of the largest ISPs in the USA. During an interview with Roger O' Crockett in 2006, Mr. Whitacre declared that companies like Google, Vonage etc. would like to do is use my pipes free, but I ain't going to let them do that because we have spent this capital and we have to have a return on it. Mr. Whitacre, with his comment about no one using his pipes for free summarised the position of ISPs –for them, it is all about profit-margins, and making sure people pay them for internet access".

of sites dependent on substance and cost will likewise influence the worldwide traffic speed and will act as a hindrance or blockage for expanding Internet utilization.

ISPs involve in shaping web traffic in the matter of unhindered internet, to earn additional profit by it. For instance, some of the ISPs brought an offer where they were permitted to charge extra from organizations administrating YouTube and Netflix platform in light of the fact that these devour more transmission capacity as compared to any general site and even these ISPs are making an offer to YouTube or Netflix in the cash that they make.

Without the principle of internet neutrality, the way we pursued the web won't be in existence, there could be "bundle plans" rather than free access for customers which definitely going to jeopardize the interest of the customers. For instance, in the event one pays Rs500, which provide services where one have the option to get to sites situated only in India and further, to access worldwide sites, one needs to pay extra charges or might have to purchase some add-on bundle services for diverse speed or for accessing other sites. The lack of an unhindered Internet will also destroy the progress of the Internet. Your ISP can charge your web organization to provide faster access to your website. Those who don't pay may see their website open slowly.

This means that large organizations like Google have the opportunity to pay more to give Internet customers access to YouTube and Google+, alternative better web for delivering videos. Most beginners who need to create a site still lack behind due to insufficient funds**.** Without the existence of this principle of net neutrality, we enter the stage of the web where it acts as a storehouse and one have to pay an extra charge or some charge to access the same to ISPs.

CONCLUSION

Since the time the Internet turned into the ordinary type of correspondence and media move, the vast majority of its clients have been underestimating it. Internet is considered as one of the most cherished mediums, this statement is based on a vote where somewhere it is recognised as compelling motivation where the internet seems like a huge development. The way the author discusses the Net Neutrality principle which has been going on now for about 10 years shows that this supposition is only an undeniable danger that lingers over, compromising the once-populist medium that comprised the interwebs.

There is no basic answer or response for the Internet Neutrality banter. The two sides of the coin the defenders and the naysayers of unhindered internet have admirable statements, however, eventually, coming to a result in a rush and settling on an off-base choice can just hamper the advancement or development of the Internet. The path forward, in any event in the Indian setting, lies in instructing the majority, presenting self-and co-administrative measures, and showing up at a thoroughly examined enactment to satisfactorily manage unhindered internet because in eyes of law everyone is at equal footing then how come one site get preference to another. It's a huge playfield where every player has an equal right to play their own fair game.

ABOUT THE EDITORS

PROF. (DR.) PRADEEP KULSHRESTHA

Prof. (Dr.) Pradeep Kulshrestha, Dean, School of Law, Sharda University is a Senior Law Academician with over 30+ years of extensive expertise in Academic. He graduated in Law from Kurukshetra University, Kurukshetra. Prof Kulshrestha received Masters in Law and a Ph.D. degree from Jodhpur University.He has been awarded Honorary Doctorate (Law) by National American University, South Dakota, USA. Prof. Kulshrestha has been awarded by various agencies of his excellent work in the field of legal aid e.g. the District Legal Service Authority (DALSA for Free Legal Aid programs, Appreciation by National Commission for Women and DCP, Women's Security, GBN, "Exemplary Academic Administrators of Higher Education Institutes across India by ULEKTZ, Chennai, Star of the Year Award by National Institute for Education & Research, New Delhi, Academic Leadership Award in Legal Education by All India Council Of Human Rights to name few. He has authored more than 8 books in the area.

PROF. (DR.) ANITA SINGH

She has more than 26 years of experience in academics, research and training. Currently She is serving at Sharda University as Professor. She has published more than 90 research articles in various refereed International/National Journals and Conference proceedings. She has been awarded with best paper awards in the International Conference on Corporate Governance: Issues, Challenges& Changing Paradigms, she has been also awarded 'Most Fabulous Professor in India' Award by WHRD Congress ,2020 and 'Indo Pacific Distinguished Professor Award 2021 by IMRF.' She has conducted and delivered session as resource person in number of FDPs and MDPs and organized National and International Seminar /Conferences. She has published three books. She is member in the Editorial and Review Board of National and International journals.

PROF. (DR.) RITU GAUTAM

Dr. Ritu Gautam, Assistant Professor, School of Law, Sharda University, is having more than 9 yr. of diverse exprience in the field of Law. Dr. Ritu has earned her Ph.D. in Cyber laws from Jiwaji University, Gwalior, Mastered in Women and Criminal laws(LLM) and Business Administration (PGDBA) from Symbiosis Pune, PGCCL in Cyber Laws from ILI. She has been active in the area of Cyber Laws, Women and Criminal Laws and ADR. Dr.Ritu is a ICADR trained mediator who is an expert in Mediation and Family Dispute Resolution, with sound experience in dealing with more than 600 cases. She has played a vital role in establishing Family Dispute Resolution Clinic (FDRC) in Greater Noida named FDRC. She has been awarded by National Commission for Women (NCW) and Utter Pradesh Police (Women and Safety wing) for her excellent work. Her previous books have received many accolades in the academic circle.

9 788195 653300